Jurnal Penelitian Sains Teknologi

Influence of Perceived Security and Perceived Risk on Continuance Intention in Using ShopeePay Digital Wallet Service: SEM-PLS Analysis

Devita Rizqi Maulida[1], Nirma Ayu Suryaningtyas[2], Selvalentina Rista Anggita[3], Umi Mahmudah[4]

[1-4]Faculty of Islamic Economics and Business, UIN K.H Abdurrahman Wahid Pekalongan, Indonesia

doi: 10.23917/saintek.v2i1.13562
Received: December 10th, 2025 | Revised: February 2nd, 2026 | Accepted: February 11th, 2026
Available Online: February 12th, 2026 | Published Regularly: March, 2026

Abstract

The rapid growth of digital payment services in Indonesia has increased the adoption of digital wallets, including ShopeePay. While the integration of technologies associated with the Fourth Industrial Revolution enhances transaction efficiency and convenience, it also raises concerns regarding security and data protection. This study examines the effects of perceived security and perceived risk on users' continuance intention to use ShopeePay. A quantitative approach was employed using Structural Equation Modeling–Partial Least Squares (SEM-PLS). Data were collected through questionnaires distributed to 76 ShopeePay users. The analysis involved evaluation of both the measurement model (outer model) and the structural model (inner model). The results indicate that all constructs meet the criteria for convergent validity and reliability, although the risk construct shows relatively lower internal consistency. Structural model analysis reveals that perceived security has a positive and significant effect on continuance intention, with a strong effect size. In contrast, perceived risk does not significantly influence continuance intention and is not significantly affected by perceived security. These findings suggest that security is a more dominant factor than risk in shaping continued use of ShopeePay. The study provides practical implications for digital payment providers to strengthen security systems and enhance communication regarding data protection, while contributing to the literature on continuance intention in fintech services.

Keywords: data protection, digital payment, information security, ShopeePay, user trust.

Corresponding Author:
Devita Rizqi Maulida, Faculty of Islamic Economics and Business, UIN K.H Abdurrahman Wahid Pekalongan
Email: devitarmlda@gmail.com

Introduction

The development of information and communication technology over the past decade has driven significant transformation in the global financial sector, including in Indonesia. The growth of digital payment services has demonstrated a rapid upward trend, in line with increasing internet penetration, smartphone adoption, and shifts in consumer behavior toward cashless transactions [1]. The increasingly mature digital economic ecosystem has positioned digital wallets (e-wallets) as one of the primary instruments supporting financial inclusion and payment system efficiency. One platform that plays a dominant role in Indonesia's digital payment ecosystem is ShopeePay, a digital wallet service directly integrated with the Shopee e-commerce platform [2].

ShopeePay offers various transaction features relevant to modern societal needs, including online payments, peer-to-peer fund transfers, mobile credit and bill purchases, and in-store payments through QR code scanning. The integration of digital financial services with the e-commerce ecosystem positions ShopeePay not only as a payment instrument but also as part of a data-driven and user experience–oriented business strategy [3]. The utilization of technologies within the framework of the Fourth Industrial Revolution such as cloud computing, big data analytics, artificial intelligence, and API-based integrated systems enables the service to operate rapidly, efficiently, adaptively, and practically [4], [5]. From a positive perspective, this transformation contributes to transaction efficiency, expanded access to financial services, and accelerated national economic digitalization.

However, digital technological advancement is inseparable from serious challenges, particularly in the areas of information security and personal data protection. The increasing complexity of digital systems corresponds directly with an expanding attack surface that can be exploited by cybercriminals [6]. In the context of digital payment systems, one of the most critical risks is the potential leakage of user data. Personal and financial information such as names, phone numbers, email addresses, transaction histories, and account details constitutes high-value assets vulnerable to hacking, identity theft, and criminal misuse. Several data breach incidents in Indonesia in recent years indicate that data protection remains an urgent issue requiring serious attention from regulators, service providers, and users [7].

This situation creates a paradox in the development of financial technology. On one hand, innovations associated with the Fourth Industrial Revolution provide convenience, speed, and comfort for users. On the other hand, broader system integration, large-scale data utilization, and reliance on digital infrastructure increase the potential for cybersecurity risks. According to Tan et al. [8], services such as ShopeePay involve real-time data processing, cross-platform integration, and intelligent analytics technologies that may create security vulnerabilities if not supported by strong information security governance, adequate data encryption, and strict access control mechanisms. In other words, the technological advancement that constitutes the primary strength of digital payment services can simultaneously become a source of vulnerability if data protection aspects are not managed comprehensively [9].

Within this framework, it is important to examine scientifically the extent to which the implementation of Fourth Industrial Revolution technologies in the ShopeePay system correlates with user perceptions and the potential risk of data breaches. In line with research conducted by Abas & Puspawati [10], such investigation is relevant because most previous studies have tended to emphasize technology adoption, user satisfaction, or ease of use in fintech services, while the dimension of data security risk has often been discussed only conceptually or from the technical perspective of system providers. In fact, users' perceptions of data security have direct implications for trust, continuance intention, and the overall stability of the digital financial ecosystem [11], [12].

This study adopts a user-centered perspective, positioning users as the primary actors in the digital payment ecosystem. Using a quantitative approach through questionnaire distribution to ShopeePay users, this research explores user perceptions, levels of concern, and experiences related to data security and potential information leakage [13]. This approach enables the identification of empirical relationships between the intensity of Fourth Industrial Revolution–based digital technology utilization and users' perceptions of data security risk. Accordingly, this study examines risk not only from the technical system perspective but also from the psychological and behavioral dimensions of users as part of digital risk management.

The novelty of this research lies in integrating two domains that are often examined separately: the adoption of Fourth Industrial Revolution–based financial technology and the risk of user data breaches within a specific digital wallet platform, namely ShopeePay. This study specifically maps how technological advancements that constitute a competitive advantage may simultaneously be perceived as sources of risk by users. Furthermore, the focus on the Indonesian context provides important contextual contributions, considering that user characteristics, levels of digital literacy, and the dynamics of data protection regulations in Indonesia possess unique features compared to other countries [14].

Practically, the findings of this study are expected to provide insights for digital payment service providers in designing security strategies that are not only technically robust but also capable of enhancing users' sense of security. For regulators and policymakers, the findings may serve as a basis for formulating personal data protection policies that are more adaptive to financial technology developments. For academics, this research enriches the literature on the relationship between digital transformation, user trust, and information security risk management within the digital financial ecosystem.

Therefore, this study aims to analyze the relationship between the implementation of Fourth Industrial Revolution technologies and the risk of data breaches in the ShopeePay digital payment system, while providing a comprehensive overview of the balance between technological innovation benefits and the challenges of user data protection in the digital economy era.

Method

This study employs a quantitative approach using the Structural Equation Modeling–Partial Least Squares (SEM-PLS) analytical method. SEM-PLS is a variance-based multivariate statistical technique used to analyze simultaneous relationships among latent variables through structural equation modeling [15]. This method was selected because it is suitable for predictive and exploratory research, capable of handling models with multiple constructs and indicators, and robust for relatively small sample sizes and non-normally distributed data.

In general, SEM-PLS analysis consists of two main stages: evaluation of the measurement model (outer model) and evaluation of the structural model (inner model) [16]. The outer model is used to assess the quality of the instrument in measuring latent constructs through validity and reliability testing, whereas the inner model is used to examine the strength of causal relationships among latent constructs in the research model.

In the study by Kartawinata et al. [17], the analyzed latent constructs include security, perceived risk, satisfaction, and continuance intention in the use of ShopeePay services. These constructs are assumed to have structural relationships in which perceived security and perceived risk influence user satisfaction, which subsequently affects continuance intention. The use of SEM-PLS aims to test both direct and indirect effects among these variables simultaneously within an integrated model.

The research was conducted in three main stages: identification, data collection and processing, and analysis and conclusion drawing.

a. Identification Stage

The initial stage involved identifying the research problem based on the phenomenon of digital payment service usage and data security issues, formulating research objectives, determining the analytical method, and developing the research instrument. The instrument was designed as a structured questionnaire based on indicators representing each latent construct.

b. Data Collection and Processing Stage

1. Data Collection

The data used in this study are primary data obtained through online questionnaire distribution on June 8, 2025. A total of 76 respondents participated, with the majority being university students as active users of digital payment services.

The questionnaire consisted of demographic data (timestamp, gender, and respondent profile) and items measuring:

- Duration of ShopeePay usage
- Frequency of transactions using ShopeePay
- Perceptions of dual security features
- Notifications of suspicious activity
- Perceptions of the technology used by ShopeePay
- Technology 4.0–based security system standards
- Security system upgrades
- Experience receiving suspicious activity notifications
- Level of concern regarding personal data breaches
- Respondents' knowledge of data security
- Satisfaction with ShopeePay's security system
- Trust in ShopeePay

These items represent the constructs of security, perceived risk, satisfaction, and continuance intention. Each statement was measured using a Likert scale.

The total of 76 respondents is considered adequate for predictive SEM-PLS analysis and exceeds the minimum requirement for basic instrument testing, such as validity and reliability testing, which generally requires at least 30 respondents (Bujang et al., 2024).

2. Data Processing

Data processing was conducted in two main stages: instrument testing and SEM-PLS analysis.

a) Instrument Testing

Before structural model analysis, instrument quality was assessed through:

1) Validity Testing

Validity testing aims to evaluate the extent to which questionnaire items represent the measured constructs. An instrument is considered valid if each indicator demonstrates adequate correlation with its corresponding latent construct.

2) Reliability Testing

Reliability testing is used to measure the internal consistency of the instrument. A construct is considered reliable if it produces consistent measurement results under relatively similar conditions [14].

b) SEM-PLS Analysis

SEM-PLS analysis in this study was conducted using the Python programming language. Python was chosen due to its open-source nature, flexibility, and interoperability with various data analysis libraries such as pandas, numpy, and scipy, thereby supporting integration in research data processing and engineering (Igolkina & Meshcheryakov, 2020).

Evaluation in SEM-PLS includes:

1) Measurement Model Evaluation (Outer Model)

This evaluation ensures that the indicators accurately measure the intended latent constructs. The criteria include:

- Convergent Validity, indicated by loading factors > 0.70
- Discriminant Validity, evaluated through cross-loading values and comparison of the square root of AVE
- Internal Consistency Reliability, measured using Composite Reliability (> 0.70) and Cronbach's Alpha (Saputra, 2018)

2) Structural Model Evaluation (Inner Model)

This evaluation examines the relationships among latent constructs in the structural model. The analyzed indicators include:

- Coefficient of Determination (R^2) to assess the ability of exogenous variables to explain endogenous variables
- Path Coefficients to determine the direction and strength of relationships among variables
- T-statistics (through bootstrapping procedures) to test the significance of relationships
- Predictive Relevance (Q^2) to assess the model's predictive capability
- Effect Size (f^2) to measure the magnitude of the influence of each exogenous variable on endogenous variables (Mardiana & Faqih, 2019)

c. Analysis and Conclusion Stage

The final stage involved analyzing the SEM-PLS modeling results to interpret the relationships among security, perceived risk, satisfaction, and continuance intention. The findings were used to address the research questions and formulate conclusions regarding the factors influencing continuance intention in using ShopeePay from the perspectives of security and data risk.

Result and Discussion

The initial stage of analysis was conducted by testing the quality of the questionnaire instrument before estimating the SEM-PLS structural model. This instrument testing aimed to ensure that each question item validly and reliably represented the measured latent constructs. Based on the results of the validity test using item–total correlation, all indicators within the Security, Risk, and Continuance constructs demonstrated r-calculated values greater than the r-table value; therefore, all items were declared valid and suitable for subsequent analysis.

Furthermore, the reliability test indicated that the Security construct (5 items) and the Continuance construct (2 items) achieved Cronbach's Alpha values ≥ 0.7, reflecting good internal consistency. Meanwhile, the Risk construct (2 items) obtained a Cronbach's Alpha value ≤ 0.7, indicating moderate internal reliability. However, in exploratory research with a limited number of indicators, such values remain acceptable as long as the other indicators demonstrate adequate measurement consistency [18]. Therefore, all indicators were retained for SEM-PLS analysis.

After confirming the adequacy of the instrument, the next stage involved constructing the main SEM-PLS model based on nine compiled questionnaire items. The evaluation of the measurement model (outer model) was performed using the PLS algorithm to obtain outer loading values, Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE) [19]. The analysis began with testing convergent validity by examining the outer loading values, as presented in Table 1.

Table 1. Outer Loadings Values

	Safety (KM)	Risk (RS)	Continuance (KB)
KM 1	0.803		
KM 2	0.822		
KM 3	0.850		
KM 4	0.648		
KM 5	0.745		
RS 1		0.843	
RS 2		0.845	
KB 1			0.861
KB 2			0.897

The general criterion states that an indicator satisfies convergent validity if the outer loading value is ≥ 0.7. However, for exploratory research, values between 0.6–0.7 are still considered acceptable [20]. Based on Table 1, all indicators within the Security (KM), Risk (RS), and Continuance (KB) constructs exhibit outer loading values above 0.6. The highest values are observed for indicators KB2 (0.897) and KB1 (0.861), indicating that the continuance indicators have very strong representational power for their construct.

Within the Security construct, most indicators demonstrate values above 0.7, except for KM4 (0.648), which remains within the acceptable threshold for exploratory research. Meanwhile, the Risk indicators (RS1 and RS2) show high values of 0.843 and 0.845, respectively, indicating strong contributions to the Risk construct. Therefore, based on Table 1, the measurement model satisfies the criteria for convergent validity.

The next stage involves evaluating construct reliability and further convergent validity using Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE), as presented in Table 2 and visualized in Figure 1. The Security construct shows a

Cronbach's Alpha value of 0.825, Composite Reliability of 0.883, and AVE of 0.604. All these values exceed the recommended minimum thresholds of 0.7 for reliability and 0.5 for AVE, indicating that the Security construct demonstrates good internal consistency and convergent validity.

Table 2. Reliability and Validity Constructs

Construct	Cronbach Alpha	Composite Reliability	AVE
Security	0.825	0.883	0.604
Risk	0.597	0.832	0.713
Continuance	0.704	0.872	0.773

The Risk construct shows a Cronbach's Alpha value of 0.597, which is slightly below the 0.7 threshold. This value indicates that the internal consistency among the Risk indicators is not as strong as that of the other constructs. Nevertheless, the Composite Reliability value of 0.832 and the AVE value of 0.713 indicate that, overall, the construct still demonstrates adequate composite reliability and convergent validity. This condition can be explained by the fact that the Risk construct consists of only two indicators, which statistically tend to produce lower Cronbach's Alpha values [18]. Therefore, the Risk construct was retained in the model, as it satisfies alternative reliability criteria through Composite Reliability.

Meanwhile, the Continuance construct demonstrates strong results, with a Cronbach's Alpha of 0.704, Composite Reliability of 0.872, and AVE of 0.773. According to Libório et al. [21], a high AVE value indicates that a substantial proportion of indicator variance is explained by the latent construct, signifying very good measurement quality. The visualization in Figure 1 shows that all constructs exhibit high composite reliability values, reinforcing the conclusion that the measurement model is generally in a good category.

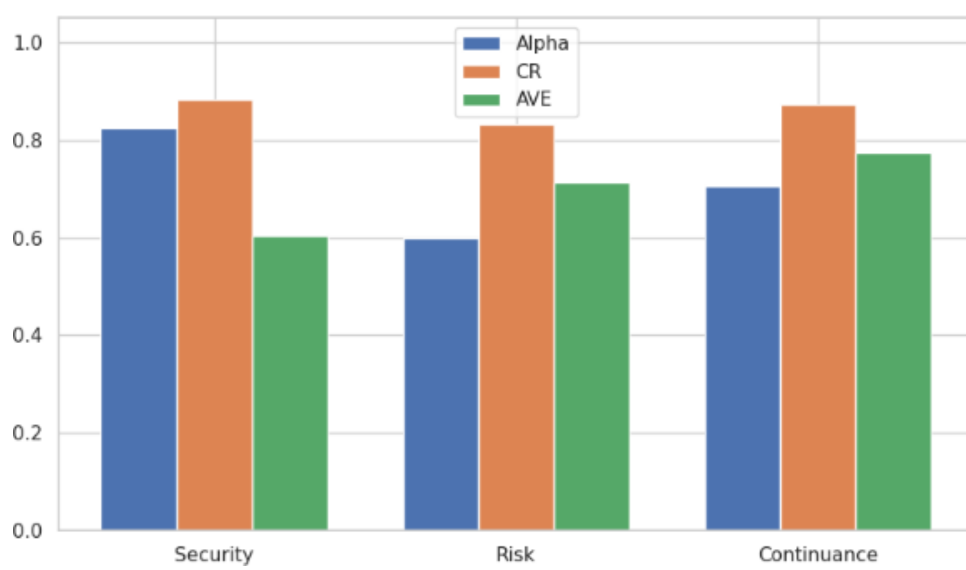

Figure 1. Reliability and Construct Validity

Overall, the results of the outer model evaluation indicate that all constructs meet the requirements for convergent validity and construct reliability, with minor considerations regarding the Risk construct that remain acceptable within the context of exploratory research. These findings suggest that the indicators used are capable of adequately representing the latent variables of Security, Risk, and Continuance. With these measurement criteria satisfied, the SEM-PLS structural model can proceed to the inner model evaluation stage to examine the causal relationships among constructs.

The results also indicate that users' perceptions of security and service continuance exhibit relatively stable measurement structures, whereas the perception of risk may require the development of more diverse indicators in future research. Based on Table 1, Table 2, and Figure 1, the measurement model in this study is deemed appropriate and meets SEM-PLS analytical standards for exploratory research [18], [20].

After confirming that the measurement model (outer model) satisfies validity and reliability criteria, the next stage involves evaluating the structural model (inner model) using the Partial Least Squares (PLS) approach. This evaluation aims to test the causal relationships among latent constructs in the research model, particularly the effects of Security and Risk on Continuance, as well as the relationship between Security and Risk. The primary parameters analyzed include path coefficients, t-statistics, and p-values, as presented in Table 3 and visualized in Figure 2.

Table 3. Inner Model (Path Coefficient)

Path	Original Sample	Sample Mean	Std Dev	t-Stat	p- value
Security – Risk	0.255	0.254	0.159	1.599	1.098
Security – Countinuance	0.689	0.691	0.091	7.525	5.262
Risk – Countinuance	0.034	0.030	0.083	0.420	6.743

Based on Table 3, the path Security → Risk shows a coefficient value of 0.255 with a t-statistic of 1.599. This value falls below the threshold for statistical significance ($t < 1.96$ at $\alpha = 0.05$), indicating that the effect of Security on Risk is not significant. In other words, the perceived security experienced by respondents does not directly reduce or increase their perception of risk in a statistically meaningful manner.

This finding suggests that even when users perceive the system as having certain security features, such perceptions do not necessarily alter their views regarding potential threats or data breaches. From a psychological perspective, risk perception may be influenced by other factors, such as personal experience, exposure to news about data breaches, or the level of digital literacy.

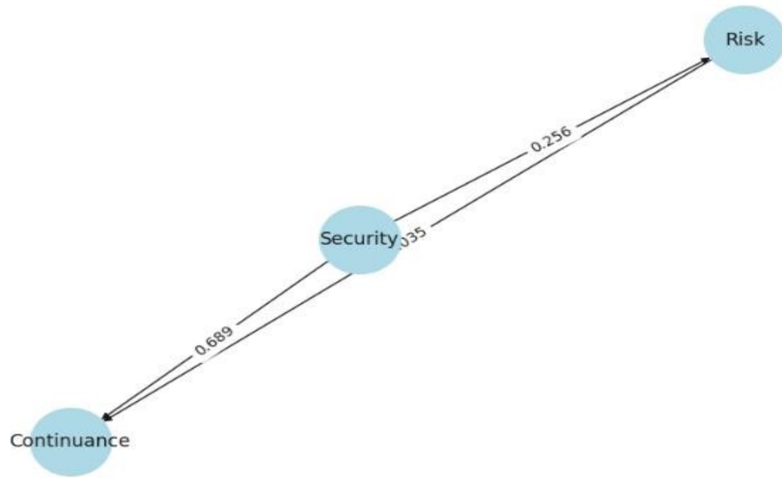

Figure 2. Inner Model (Path Coefficient)

The second path, Security → Continuance, demonstrates markedly different results. The path coefficient of 0.689 with a t-statistic of 7.525 indicates a strong and statistically significant effect. This result is also clearly illustrated in Figure 2, where the directional weight from Security to Continuance is the largest among all paths in the model. These findings confirm that perceived security is the primary determinant driving users' intention to continue using ShopeePay. The higher the users' confidence in the system's security, the greater the likelihood that they will maintain long-term usage. This result is consistent with trust theory in information systems, which posits that a sense of security is a fundamental prerequisite for the formation of continuance intention in technology-based services.

In contrast, the Risk → Continuance path shows a very small coefficient of 0.034 with a t-statistic of 0.420, indicating a non-significant effect. This suggests that perceived risk does not have a meaningful direct influence on continuance intention. Although risk is theoretically assumed to reduce usage intention, in the context of this study, it does not appear to be a primary consideration in users' decisions to continue using ShopeePay [22]. It is likely that functional benefits and service convenience are more dominant than concerns about risk, particularly among respondents largely composed of younger individuals who are accustomed to digital technologies.

Overall, the inner model results presented in Table 3 and Figure 2 confirm that Security is the key variable directly influencing Continuance, whereas Risk is not proven to play a significant role, either as a direct independent variable or as a mediator [23]. These findings suggest that strategies aimed at enhancing continued usage of digital payment services should prioritize strengthening security features and communicating security aspects effectively, rather than focusing solely on reducing perceived risk.

In addition to testing path significance, the inner model was further evaluated through effect size (f^2) analysis to determine the magnitude of each exogenous variable's contribution to endogenous variables. The f^2 values are categorized as small (0.02), medium (0.15), and large (0.35). The effect size calculation results are presented in Table 4 and further supported by the visualization of correlations among constructs in Figure 3.

Table 4. Effect Size of Relationships Between Constructs

Effect	f2	Interpretation
Security – Risk	0.048	Low
Security – Countinuance	0.871	Strong
Risk – Countinuance	0.003	Very Low

Based on Table 4, the Security → Risk path has an f² value of 0.048, which falls into the small effect size category. This indicates that although the direction of the relationship is positive, the contribution of Security in explaining the variance of Risk is relatively limited. This finding is consistent with the previous significance test results, which showed that this relationship is not statistically significant.

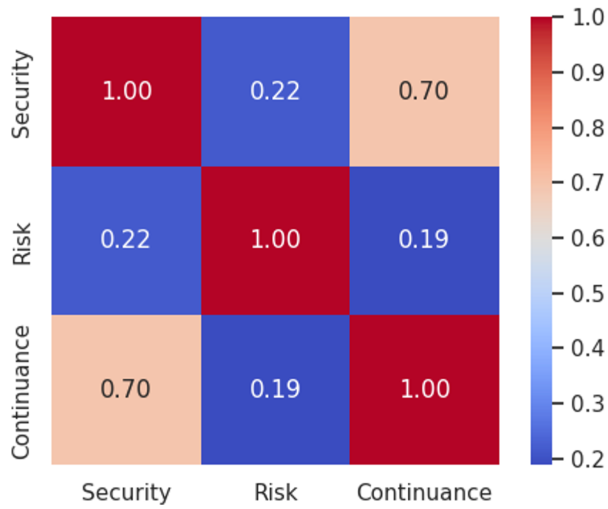

Figure 3. Correlation Between Constructs

In contrast, the Security → Continuance path shows an f² value of 0.871, which falls into the strong effect size category. This value substantially exceeds the threshold for a large effect (0.35), thereby confirming that Security is the dominant predictor of Continuance. The visualization in Figure 3 also illustrates the thickest or strongest correlation along this path. These results reinforce the earlier interpretation that security is a strategic factor in sustaining user loyalty and continued service usage.

Meanwhile, the Risk → Continuance path has an f² value of 0.003, which is categorized as extremely small. This indicates that the contribution of Risk to Continuance is practically negligible. Although risk is frequently emphasized in the information security literature, in the context of ShopeePay usage among the respondents in this study, risk does not serve as a primary determinant of continuance behavior. This finding aligns with previous studies suggesting that in digital services integrated into daily needs, perceived benefits and convenience often outweigh concerns about risk [24], [25].

Based on Table 3, Figure 2, Table 4, and Figure 3, it can be concluded that Security is the most influential factor in driving continuance intention in using ShopeePay, both in terms of statistical significance and effect size. In contrast, Risk does not demonstrate a meaningful influence and therefore does not function as a key determinant in the structural model of this study. These findings imply that service providers should prioritize strengthening security systems while effectively communicating these aspects to users in order to enhance user retention and loyalty.

Conclusion

This study aims to analyze the relationships among perceived security, perceived risk, and continuance intention in using the ShopeePay digital payment service by employing the Structural Equation Modeling–Partial Least Squares (SEM-PLS) approach. Based on the evaluation of the measurement model (outer model), all examined constructs Security, Risk, and Continuance meet the criteria for convergent validity and construct reliability. Although the Risk construct has a Cronbach's Alpha value slightly below the ideal threshold, its Composite Reliability and AVE values indicate that it remains acceptable for retention in an exploratory research model.

The results of the structural model (inner model) evaluation reveal that Security is the most significant and dominant variable influencing Continuance. The high and statistically significant path coefficient, supported by a strong effect size, confirms that users' perceptions of ShopeePay's security system play a crucial role in shaping their intention to continue using the service. In other words, the greater the users' trust in the implemented security mechanisms, the stronger their tendency to sustain long-term usage.

In contrast, Risk is not found to have a significant effect on Continuance, either directly or through its relationship with Security. Furthermore, the influence of Security on Risk is also not significant. These findings suggest that, within the context of this study, perceived risk is not a primary factor affecting users' decisions to continue using ShopeePay. This may be attributed to the characteristics of respondents who are relatively accustomed to digital technologies, where functional benefits and service convenience outweigh concerns regarding data security risks.

Overall, this study confirms that within the digital payment ecosystem, security serves as a key determinant in fostering continuance intention, whereas perceived risk does not necessarily function as a primary barrier. Practically, these findings imply that fintech service providers should prioritize strengthening security infrastructure, ensuring transparency in data protection systems, and effectively communicating security features to users.

From an academic perspective, this research contributes by demonstrating that the relationships among security, risk, and continuance intention in digital services are contextual and not always linear, as assumed in some technology adoption models. Therefore, future research is recommended to develop more comprehensive risk indicators, involve more diverse samples, and consider additional variables such as trust and perceived usefulness to obtain a more holistic understanding of continuance behavior in digital payment services.

Reference

[1] A. Thommandru and B. Chakka, "The Globalization of Cashless Transactions Using Blockchain Technology to Preventing Money Laundering and The Changing Trends in The Cryptocurrency Market: A Learning Experience of Polish and EU Laws," *European Studies*, vol. 9, no. 2, pp. 213–233, Dec. 2022, doi: 10.2478/eustu-2022-0021.

[2] M. Al-Okaily, "The influence of e-satisfaction on users' e-loyalty toward e-wallet payment apps: a mediated-moderated model," *International Journal of Emerging Markets*, vol. 20, no. 6, pp. 2428–2454, May 2025, doi: 10.1108/IJOEM-08-2022-1313.

[3] B. L. Handoko, I. G. M. Karmawan, and L. Meliana, "Factors Influenced User Interest in Payment Transaction of ShopeePay Digital Wallet Application," in *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/ICORIS56080.2022.10031472.

[4] S. Sivamohan and S. S. Sridhar, "An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework," *Neural Comput. Appl.*, vol. 35, no. 15, pp. 11459–11475, May 2023, doi: 10.1007/s00521-023-08319-0.

[5] S. Jain, S. Sharma, and R. Tomar, "Integration of Wit API with Python Coded Terminal Bot," 2019, pp. 397–406. doi: 10.1007/978-981-13-1501-5_34.

[6] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *J. Intell. Manuf.*, vol. 30, no. 3, pp. 1111–1123, Mar. 2019, doi: 10.1007/s10845-017-1315-5.

[7] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," *IEEE Trans. Industr. Inform.*, vol. 15, no. 7, pp. 4362–4369, Jul. 2019, doi: 10.1109/TII.2019.2891261.

[8] V. Tan and V. N. Renata, "The effect of promotion, expenditure budgeting, and consumptive behavior on Indonesians' intention of using GoPay or ShopeePay," *E3S Web of Conferences*, vol. 426, p. 02060, Sep. 2023, doi: 10.1051/e3sconf/202342602060.

[9] Hariyadi, K. Handoko, and A. Noviliza, "The Influence of Information Technology and Communication Advancement Especially Smartphone on Muhammadiyah University of West Sumatera's Students Year 2019," *J. Phys. Conf. Ser.*, vol. 1779, no. 1, p. 012083, Feb. 2021, doi: 10.1088/1742-6596/1779/1/012083.

[10] N. I. Abas and D. Puspawati, "E-Wallet Adoption in Continuance Intention As A e-Payment System for Live Streaming Shopping," *Procedia Comput. Sci.*, vol. 234, pp. 1137–1144, 2024, doi: 10.1016/j.procs.2024.03.109.

[11] N. Widayanto, A. R. Lahitani, and N. I. Kusumaningtyas, "Analisis Keamanan Data Pribadi pada Shopee Paylater Menggunakan Metode Hybrid," *Teknomatika: Jurnal Informatika dan Komputer*, vol. 15, no. 1, pp. 28–33, May 2021, doi: 10.30989/teknomatika.v15i1.1097.

[12] K. Zhang, W. Zuo, Y. Chen, D. Meng, and L. Zhang, "Beyond a Gaussian Denoiser: Residual Learning of Deep CNN for Image Denoising," *IEEE Transactions on Image Processing*, vol.

26, no. 7, pp. 3142–3155, Jul. 2017, doi: 10.1109/TIP.2017.2662206.

[13] W. Adiani, A. Aprianingsih, I. Fachira, T. Debby, and A. P. Maharatie, "Social influence, financial benefit, and e-wallet multi-brand loyalty: The mediating impact of commitment," *Cogent Business & Management*, vol. 11, no. 1, Dec. 2024, doi: 10.1080/23311975.2023.2290228.

[14] S. K. W. Amnesti, S. Zulaichah, and N. Istiqomah, "Legal protection of personal data security in Indonesian Local Government apps: Al Farabi's perspective," *Legality : Jurnal Ilmiah Hukum*, vol. 33, no. 1, pp. 1–19, Oct. 2024, doi: 10.22219/ljih.v33i1.34623.

[15] M. Yusuf, "Pengaruh Promosi, Gaya Hidup, dan Persepsi Risiko terhadap Niat Beli Motor Listrik menggunakan Metode SEM - PLS," *G-Tech: Jurnal Teknologi Terapan*, vol. 6, no. 2, pp. 241–248, Sep. 2022, doi: 10.33379/gtech.v6i2.1685.

[16] D. Novitasari *et al.*, "Optimizing Educational Technology for Inclusive and Quality Learning Through PLS-SEM Analysis," in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*, IEEE, Aug. 2025, pp. 1–7. doi: 10.1109/ICCIT65724.2025.11167583.

[17] B. R. KARTAWINATA, A. A. WAFA, D. KURNIANINGRUM, M. Fakhri, A. WARDHANA, and R. JOVIANO, "The impact of digital marketing and brand trust on e-wallet adoption (study on ShopeePay Indonesia)," in *International Conference on Medical Imaging, Electronic Imaging, Information Technologies, and Sensors (MIEITS 2024)*, J. Jaiswal, Ed., SPIE, Jun. 2024, p. 47. doi: 10.1117/12.3032488.

[18] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," *Int. J. Med. Educ.*, vol. 2, pp. 53–55, Jun. 2011, doi: 10.5116/ijme.4dfb.8dfd.

[19] K. S. Taber, "The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education," *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1273–1296, Dec. 2018, doi: 10.1007/s11165-016-9602-2.

[20] N. H. Mohd Dzin and Y. F. Lay, "Validity and Reliability of Adapted Self-Efficacy Scales in Malaysian Context Using PLS-SEM Approach," *Educ. Sci. (Basel).*, vol. 11, no. 11, p. 676, Oct. 2021, doi: 10.3390/educsci11110676.

[21] M. P. Libório, A. M. A. Diniz, D. A. G. Vieira, and P. I. Ekel, "Subjective–Objective Method of Maximizing the Average Variance Extracted From Sub-indicators in Composite Indicators," *Soc. Indic. Res.*, vol. 175, no. 2, pp. 613–637, Nov. 2024, doi: 10.1007/s11205-024-03385-w.

[22] H. Mohd Thas Thaker, N. R. Subramaniam, A. Qoyum, and H. Iqbal Hussain, "Cashless society, e-wallets and continuous adoption," *International Journal of Finance & Economics*, vol. 28, no. 3, pp. 3349–3369, Jul. 2023, doi: 10.1002/ijfe.2596.

[23] C. Aprilia and R. Amalia, "How Perceived Security Influences Continuance Intention to Use Mobile Wallet," *Jurnal Minds: Manajemen Ide dan Inspirasi*, vol. 9, no. 2, pp. 271–288, Dec. 2022, doi: 10.24252/minds.v9i2.30083.

[24] M. S. Adhantoro *et al.*, "Hybrid Deep-Ensemble Learning for Cybersecurity: A Multi-Dataset Framework Achieving High Precision and Minimal False Positives in Attack Detection," *International Journal of Intelligent Engineering and Systems*, vol. 18, no. 8, pp. 692–706, Sep. 2025, doi: 10.22266/ijies2025.0930.42.

[25] Y.-M. Wang and Y.-X. Li, “Adaptive security control of time-varying constraints nonlinear cyber-physical systems with false data injection attacks,” *Journal of Control and Decision*, vol. 11, no. 1, pp. 50–59, Jan. 2024, doi: 10.1080/23307706.2022.2136274.