



contact: +62 813 266 9393 or admin@adicita.org

JOSEM: Journal of Sustainable and Economic Management

<http://josem.adicita.org/josem>



The Role of Privacy in Mediating the Use of GoPay Biometrics in Financial Transactions

Silviana¹, Citra Ayudiati²

Department of Accounting, Faculty of Economics and Business, Universitas Cokroaminoto Yogyakarta,
Indonesia^{1,2}

Article History:

Received : 2026-02-05
Revised : 2026-03-10
Accepted : 2026-03-30
Published : 2026-05-01

Keywords:

GoPay; Digital wallet; Biometric authentication; Privacy; Fintech adoption

Corresponding author:

Silviana

Author's email:

silvianna@gmail.com

Paper type:

Research

Abstract

Purpose – This study aims to examine the role of privacy in mediating the influence of trust, convenience, perceived value, and security on the intensity of biometric-based digital wallet usage, with GoPay as the case study.

Methodology – This study used an explanatory quantitative design through purposive sampling of 105 GoPay users who use fingerprint authentication. Respondents remained anonymous because personal identities were not collected or recorded, thus ensuring confidentiality and voluntary participation. Data were analyzed using Partial Least Squares–Structural Equation Modeling (PLS-SEM) with SmartPLS 3.0 to evaluate the reliability, validity, and structural relationships between the research variables.

Findings – The results show that convenience, perceived value, and security have a positive and significant effect on privacy perceptions, while trust has no significant effect on privacy. Privacy has a strong and significant effect on usage intensity, confirming its role as the main mediating variable in the research model. Higher privacy perceptions encourage more intensive use of biometric-based digital wallets.

Implications – These findings have managerial implications for fintech providers to strengthen privacy protection through enhanced security systems, user-friendly application design, and transparent data governance in order to increase user engagement and sustainable use of biometric based digital payment services.

Originality – This study integrates the Technology Acceptance Model (TAM), UTAUT2, and Privacy Calculation Theory into a framework to explain the use of biometric-based digital wallets. Focusing on GoPay users in Indonesia, this study provides empirical insights into the mediating role of privacy in fintech adoption.

Introduction

The rapid development of financial technology (fintech) has transformed digital payment systems into a key infrastructure in both business activities and daily life. In Indonesia, the adoption of digital wallets such as GoPay has grown significantly, supported by biometric authentication innovations, particularly fingerprint verification, which provide users with both security and convenience (Sahabuddin et al., 2025). Nevertheless, the implementation of biometric features still faces challenges, especially regarding trust, privacy, and data security, which play a crucial role in shaping user behavior toward digital financial services (Hanifah et al., 2025).

Trust is a fundamental factor driving adoption and continuous use of digital wallets. In the context of GoPay, trust reflects users' confidence in the reliability, security, and integrity of the platform in protecting sensitive data, including biometric information such as fingerprints (Faridah & Kuswati, 2024). Recent studies

emphasize that secure systems and seamless authentication processes strengthen user trust and ultimately enhance usage intensity ([Prawira et al., 2024](#)). Conversely, perceived risks of misuse or leakage of personal data decrease trust levels, thereby discouraging adoption even when the system offers functional advantages ([Hanifah et al., 2025](#)).

Another determinant is convenience, which refers to the ease with which users operate applications and perform transactions. Fingerprint authentication accelerates verification, reduces cognitive effort, and enhances overall user experience ([Ismail et al., 2023](#)). This aligns with the Technology Acceptance Model (TAM), which states that perceived ease of use positively influences technology adoption ([Simanjuntak et al., 2024](#)). Empirical findings also highlight that applications with simple interfaces and seamless processes tend to increase user satisfaction and loyalty ([Liébana-Cabanillas et al., 2024](#)).

Perceived value also plays a crucial role. It reflects the extent to which users weigh the benefits of a service against its costs, risks, or efforts. In digital financial services, assurance of security, accessibility, and ease of use strongly influence perceived value and strengthen behavioral intention to adopt the system ([Mulyawan & Sharif, 2022](#)). Within biometric authentication, efficiency, comfort, and hedonic motivation also contribute to perceived value, thereby encouraging continued usage ([Wang, 2025](#)).

Security remains a central issue shaping user trust in digital payment systems. Fingerprint verification provides an additional layer of protection that is more difficult to manipulate than traditional methods such as PINs or passwords ([Jannah et al., 2024](#)). This mechanism reduces the risk of fraud and unauthorized access, including cyber threats such as SIM-swap and account takeovers ([Hassan & Shukur, 2022](#)). Furthermore, platforms such as GoPay have implemented broader cybersecurity mechanisms, including encryption, multi-factor authentication, and real-time transaction monitoring, to ensure system reliability ([Mulyana, 2025](#)).

Despite these efforts, privacy perception remains a primary concern among users of biometric-based digital services. Privacy refers to users' confidence that their biometric data is protected and not misused in digital transactions ([Rhois et al., 2024](#)). Although technically digital wallet providers do not store fingerprint data because it is managed by the device's secure enclave, privacy perception still significantly affects usage intensity. Studies show that privacy concerns act as a mediating variable linking trust, security, and convenience to behavioral intention ([Khoiriah et al., 2025](#)). When privacy perception is high, users are more likely to adopt and continuously use biometric features; when low, adoption decreases even if the system is technically secure ([Widiyanto, 2024](#)).

The Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) emphasizes that adoption is influenced by performance expectancy, effort expectancy, social influence, and facilitating conditions, with habit and hedonic motivation as moderators ([Auliano et al., 2025](#)). In the biometric context, fingerprint verification enhances effort expectancy (ease of use) and performance expectancy (security and efficiency), while social influence emerges from peers or communities adopting similar technologies. Similarly, the Privacy Calculus Theory explains that users weigh risks (such as privacy loss) against benefits (such as security and convenience) before deciding to adopt ([Rhois et al., 2024](#)). Recent studies in Indonesia confirm that when privacy assurance is effectively communicated, users tend to accept biometric features despite initial concerns ([Sasongko et al., 2021](#)).

However, prior research on biometric payment systems has shown inconsistent findings. Some studies emphasize trust and security as significant predictors of usage intensity ([Hanifah et al., 2025](#)), while others highlight the stronger role of convenience and perceived value ([Mulyawan & Sharif, 2022](#)). Similarly, while some argue that privacy concerns reduce adoption ([Widiyanto, 2024](#)), others find that such concerns can be offset if security and value are perceived as sufficiently strong ([Liébana-Cabanillas et al., 2024](#)). These inconsistencies reveal a research gap, particularly in the context of Indonesian GoPay users, whose cultural, regulatory, and technological environment differs from other countries.

Based on this gap, the objectives of this study are threefold: first, to examine the effects of trust, convenience, perceived value, and security on the intensity of biometric-based digital wallet usage; second, to analyze the mediating role of privacy perception in linking these variables to usage intensity; and third, to provide empirical evidence that complements previous studies, especially within the Indonesian context, which remains underexplored in international literature.

This study contributes to both theory and practice. Theoretically, it enriches digital finance adoption literature by integrating the Technology Acceptance Model (TAM), UTAUT2, and Privacy Calculus into a comprehensive model. Practically, it offers guidance for providers such as GoPay in formulating policies, designing

effective communication strategies, and developing stronger biometric features to enhance user trust and privacy protection.

Thus, this study is expected to provide new empirical insights that advance academic discourse while also supporting practical decision-making in digital financial technology, particularly in Indonesia, where biometric authentication in digital wallets is gaining increasing relevance and acceptance.

Literature Review

Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) model is a conceptual development of technology adoption theory that was developed through the integration of various approaches to user behavior in the field of information systems. This model is rooted in the synthesis of several major theories, such as the Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), and Innovation Diffusion Theory (IDT), which together explain the cognitive and social determinants of technology acceptance ([Liébana-Cabanillas et al., 2024](#)). UTAUT2 places the consumer context as the main focus by adding new dimensions to the original UTAUT model, namely Hedonic Motivation, Price Value, and Habit, in addition to the main constructs of Performance Expectancy and Effort Expectancy ([Widyaretno & Indriyanti, 2023](#)). In the context of biometric-based digital financial services such as GoPay, these constructs are represented through Perceived Value and Convenience, which describe the extent to which users assess the benefits, efficiency, and ease of the system in supporting digital transaction activities ([Prawira et al., 2024](#)). The higher the perception of the benefits and convenience of the service, the greater the user's intention to continue adopting the technology on an ongoing basis, which ultimately strengthens loyalty and actual behavior in the use of modern digital financial services ([Zarco et al., 2024](#)).

Trust

Trust is a key factor in determining interest and continued use of e-wallet services. Users will have more confidence in platforms such as GoPay when they are certain that their personal and biometric data is secure and that the system operates with high integrity ([Faridah & Kuswati, 2024](#); [Sahabuddin et al., 2025](#)). International research shows that perceptions of security, risk, and trust are key determinants in the adoption of biometric payment technology ([Liébana-Cabanillas et al., 2024](#); [Zarco et al., 2024](#)). Other studies also confirm that improved authentication and privacy significantly strengthen user trust in e-wallets ([Hassan & Shukur, 2022](#); [Prawira et al., 2024](#)).

H1: Trust has a positive and significant effect on privacy.

Convenience

Convenience is an important aspect in increasing user acceptance and satisfaction with digital wallet services such as GoPay. Convenience is defined as the perception that the system can be used without requiring much effort, including speed, practicality, and simplicity of the user interface. In the context of fingerprint features, convenience is evident in the efficiency of the authentication process and fast transactions without the need to manually enter a password. International research shows that perceptions of convenience and benefits have a significant effect on the intention to adopt digital financial services in emerging markets ([Kajol et al., 2022](#)). Another study in Digital Business found that ease of use is a major driver of fintech adoption because it improves user experience and satisfaction ([Sethi et al., 2025](#)). Furthermore, bibliometric research in Heliyon identifies that the integration of artificial intelligence and machine learning can strengthen the aspect of ease of use by creating more automated and user-friendly transaction processes ([Pattnaik et al., 2024](#)). Recent research in Research in International Business and Finance also confirms that the convenience of disruptive financial technology can increase accountability and user trust in digital payment systems ([Secinaro et al., 2025](#)). Thus, the ease of using GoPay's fingerprint feature not only increases transaction efficiency but also strengthens users' intentions and trust in interacting with modern financial technology.

H2: Convenience has a positive and significant effect on privacy.

Perceived Value

Perceived Value is defined as the user's overall evaluation of the benefits obtained compared to the costs, efforts, and risks incurred in using a digital service. In the context of digital payments, this value reflects the extent to which users feel the convenience, security, and efficiency are commensurate with the resources sacrificed. Previous research shows that perceived value is influenced by service attributes such as security guarantee policies, ease of use, and availability of transaction partners, which increase the perception of benefits and strengthen users' intention to continue using digital payment services ([Mulyawan & Sharif, 2022](#)). In the adoption of digital financial services, perceived usefulness and ease of use have been proven to be the main factors that shape perceived value because they provide an efficient and convenient user experience ([Wang, 2025](#)). International research also confirms that biometric technologies such as fingerprint authentication can increase perceived value by improving transaction speed, security, and user intrinsic satisfaction ([Liébana-Cabanillas et al., 2024](#)). In addition, the perception of value related to performance expectancy plays an important role in increasing the intention and frequency of using digital payment systems ([Prawira et al., 2024](#)). Thus, Perceived Value serves as an important determinant that influences user intention and loyalty towards digital payment services such as GoPay, as it reflects the belief that these services provide tangible benefits, convenience, and security that meet or even exceed user expectations.

H3: Perceived value has a positive and significant effect on privacy.

Security

Security can be understood as the extent to which users believe that digital payment systems are capable of protecting personal data, financial information, and transaction activities from various threats such as fraud, hacking, and misuse of information by unauthorized parties. In this context, security plays an important role in shaping user trust and comfort in using services such as GoPay ([Putri et al., 2024](#)). Biometric technology, such as fingerprint authentication, is a significant innovation because it provides an additional layer of protection that is stronger than conventional methods such as PINs or passwords, given that biometric characteristics are unique and difficult to forge ([Hassan & Shukur, 2022](#); [Jannah et al., 2024](#)). A reliable e-wallet system is characterized by its ability to maintain data integrity and confidentiality, as well as protect against potential loss and illegal access ([Auliano et al., 2025](#)). The implementation of modern security technologies such as data encryption, multi-factor authentication, and real-time transaction monitoring also strengthens the digital defense system ([Jannah et al., 2024](#); [Mulyana, 2025](#)). In addition, privacy also plays an integral role in security, as it reflects users' confidence that their personal and biometric data is managed ethically and in accordance with strict data protection policies ([Saputri, 2023](#)). Privacy even serves as a link between security and user behavior, where secure systems increase the perception of trust, which ultimately strengthens loyalty to digital payment services such as GoPay ([Zarco et al., 2024](#)).

H4: Security has a positive and significant effect on privacy.

Privacy

Privacy in digital financial services reflects users' perceptions of the protection of their personal data, especially biometric data such as fingerprints, which is a crucial aspect in building trust in digital payment systems. Although technically GoPay does not store biometric data because it is managed through a secure enclave on the user's device, perceptions of data security and confidentiality remain a determining factor that influences the level of trust and intention to use ([Rhois et al., 2024](#)). In the context of the UTAUT model, privacy functions as a mediating variable that bridges the relationship between performance expectations, ease of use, and facilitation conditions with actual user behavior, where concerns about potential data leaks can reduce usage intentions even though the application offers efficiency and convenience ([Khoiriah et al., 2025](#)). Increased security threats such as phishing, malware, identity theft, and SIM-swap reinforce the urgency of privacy in digital payment systems, because even though biometric authentication can reduce the risk of fraud, users still pay great attention to the protection of personal data ([Marakalala, 2023](#)). The implementation of fingerprint-based authentication combined with cryptographic encryption such as the Rivest Shamir Adleman (RSA) algorithm has been proven to increase data confidentiality and integrity. However, this technical effectiveness does not automatically guarantee user acceptance, as perceptions of privacy are the link between technological reliability and user loyalty ([Widiyanto,](#)

2024). Thus, trust in the secure management of biometric data is the main foundation that strengthens the relationship between technological reliability, security perceptions, and the behavior of using digital financial services such as GoPay.

H5: Privacy has a positive and significant effect on Intensity of Use.

Usage Intensity

The frequency and consistency of fingerprint authentication feature usage on GoPay reflects the level of user engagement and loyalty to digital financial services, while also serving as an indicator of the success of long-term financial technology adoption. Perceptions of security, privacy, ease of use, as well as social influence and habits have been shown to have a significant effect on consistency of use (Sasongko et al., 2021; Zarco et al., 2024). The high intensity of biometric feature usage indicates positive user acceptance of biometric-based payment systems, driven by a sense of security, efficiency, and trust in the technology (Auliano et al., 2025).

To better understand the development of previous research on biometric payment systems and digital wallet adoption, several relevant studies are summarized in Table 1.

Tabel 1. Summary table of previous research

Author	Variables	Method	Findings	Research Gap
Hartono et al. (2022)	Biometric security → Digital wallet transactions	Systematic Literature Review	Biometrics enhance transaction security and are difficult to forge.	Does not examine behavioral factors influencing biometric use.
Widyaretno & Indriyanti (2023)	UTAUT variables → behavioral intention	Quantitative (PLS-SEM)	Performance expectancy, convenience, and credibility increase biometric adoption.	Privacy and intensity of use were not analyzed.
Jannah et al. (2024)	Biometric authentication → security & privacy	Systematic Literature Review	Biometrics provide stronger protection than PIN/password	Limited empirical testing.
Auliano et al. (2025)	Security strategies → user trust	Literature Review	Encryption and authentication strategies increase trust in e-wallets.	Lacks empirical testing of relationships.
Faridah & Kuswati (2024)	Usefulness, security, convenience → adoption (trust mediator)	Quantitative (PLS-SEM)	Security and convenience influence adoption through trust.	Privacy as a mediator was not analyzed
Sahabuddin et al. (2025)	Convenience, security, promotion, trust → e-wallet use	Quantitative (PLS-SEM)	Convenience and trust strongly influence usage.	Biometric security factors not included.
Khoiriah et al. (2025)	System security → privacy	Systematic Literature Review	Digital finance faces threats such as phishing and malware.	Limited discussion of user behavior.
Zarco et al. (2024)	Risk, social influence, trust → biometric payment intention	Mixed Method	Risk perception and social influence drive biometric adoption.	Limited sample size and lack of cross-cultural analysis.

Author	Variables	Method	Findings	Research Gap
Prawira et al. (2024)	Authentication, encryption, privacy → continuance intention	Quantitative (PLS-SEM)	Security factors increase satisfaction and continued use.	Convenience and perceived value not integrated.
Sasongko et al. (2021)	Usefulness, ease of use, trust, security → continuance intention	Quantitative (PLS-SEM)	Trust and usefulness significantly influence sustainable use.	Biometric authentication is not checked

Based on a summary of previous research in Table 1, most studies focus on technological security aspects, e-wallet adoption, and factors that influence the intention to use digital financial services. However, there are still limitations in research that simultaneously examines the influence of trust, convenience, perceived value, and security on privacy and its impact on usage intensity in the use of biometric features in e-wallet services. Therefore, this study aims to fill this research gap by analyzing the relationship between these variables in the use of fingerprint features in GoPay services.

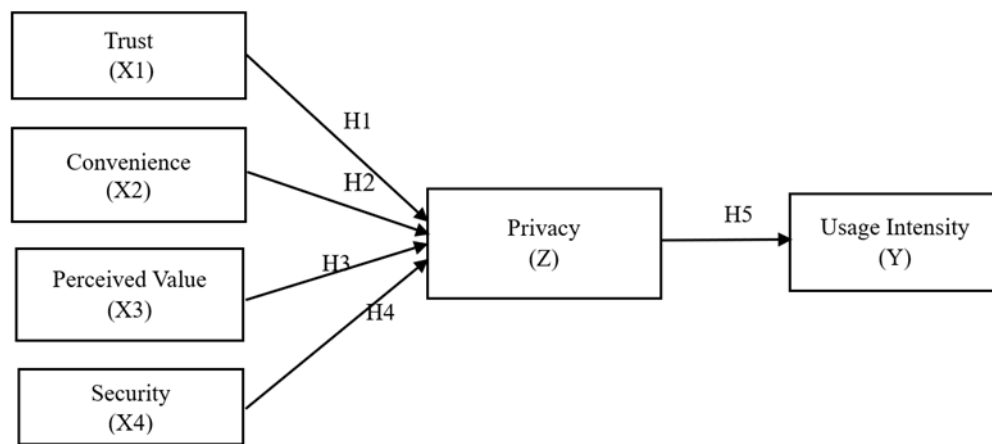


Figure 1. Research Model

Research Methods

This study employs a quantitative approach with an explanatory design. This approach was selected because the objective of the research is to examine causal relationships among the latent variables of trust, convenience, perceived value, security, privacy, and usage intensity in the context of biometric-based GoPay usage in Indonesia. A quantitative method is considered appropriate since it enables hypotheses to be tested objectively through statistical analysis, thereby allowing generalization of the findings to a broader population. The explanatory design was particularly relevant as the study aims to provide empirical evidence on the interrelationships between the variables rather than merely describing the phenomenon.

The population of this study comprises all GoPay users in Indonesia. Given the large and dispersed population, the research adopted a purposive sampling technique with specific criteria: respondents must be active GoPay users and must have utilized biometric authentication features, specifically fingerprint verification. Based on these criteria, a total of 105 anonymous respondents were collected. This sample size is considered adequate, as it meets the minimum requirement for Partial Least Squares Structural Equation Modeling (PLS-SEM), which generally requires five to ten times the number of indicators used in the measurement model. Consequently, the sample is methodologically sufficient to ensure validity and reliability of the findings.

The data in this study was collected through an online questionnaire distributed using the Google Forms platform. The questionnaire instrument was divided into two main sections. The first section contained questions about the demographic characteristics of the respondents, such as age, education level, length of GoPay usage, and frequency of use of the service. The second section contained a number of statements to measure six research variables, namely Trust (T), Convenience (C), Perceived Value (PV), Security (S), Privacy (P), and Usage Intensity (UI). All statement items were measured using a four-point Likert scale with a range of values from 1 = strongly disagree to 4 = strongly agree. The use of a four-point scale aims

to minimize the tendency of respondents to choose neutral answers (central tendency bias) and encourage respondents to give more decisive assessments of each statement.

Each research variable is operationalized through a number of indicators adapted from previous studies. The Trust variable is measured using four indicators, namely system reliability, service provider integrity, personal data protection, and service transparency, which are adapted from ([Hanifah et al., 2025](#); [Faridah & Kuswati, 2024](#); [Prawira et al., 2024](#); [Sahabuddin et al., 2025](#)). The Convenience variable is measured using four indicators, including ease of access, transaction speed, interface simplicity, and verification process efficiency, which are adapted from ([Liébana-Cabanillas et al., 2024](#); [Putri et al., 2024](#); [Simanjuntak et al., 2024](#); [Ismail et al., 2023](#)).

Perceived Value Variables are measured using five indicators, namely perceived usefulness, perceived ease of use, perceived transaction security, availability of transaction partners, and hedonistic motivation. These indicators are adapted from ([Kusuma et al., 2021](#); [Mulyawan & Sharif, 2022](#); [Wang, 2025](#); [Zarco et al., 2024](#)). The Security variable was measured using four indicators consisting of personal data protection, biometric authentication, system encryption, and real-time transaction monitoring, which were adapted from ([Hassan & Shukur, 2022](#); [Jannah et al., 2024](#); [Mulyana, 2025](#); [Putri et al., 2024](#)).

The Privacy variable was measured using four indicators, namely perception of data protection, concern about potential data leaks, compliance with privacy protection regulations, and the level of trust in biometric data management, adapted from ([Marakalala, 2023](#); [Rhois et al., 2024](#); [Khoiriah et al., 2025](#); [Widiyanto, 2024](#)). Meanwhile, the Usage Intensity variable is measured using four indicators, which include frequency of use, consistency of use, continuance use intention, and loyalty to the fingerprint feature, adapted from ([Abdul-Halim et al., 2022](#); [Franque et al., 2021](#); [Sasongko et al., 2021](#); [Zarco et al., 2024](#)). Overall, this research instrument consists of 25 statement items used to measure the six research variables. The content validity of the instrument was tested through expert judgment, while the construct validity and reliability were tested at the outer model evaluation stage in Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis.

Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) with the assistance of SmartPLS version 3.0. This method was chosen for several methodological reasons: (1) PLS-SEM is suitable for relatively small sample sizes, (2) it does not require normally distributed data, and (3) it is capable of analyzing complex structural models with multiple latent constructs. The analysis was carried out in two stages. The outer model evaluation was conducted to test the validity and reliability of the indicators through convergent validity, discriminant validity, composite reliability, and Cronbach's Alpha. The inner model evaluation was then performed to examine the structural relationships among latent variables, using R^2 values to assess predictive power and the bootstrapping procedure to test the significance of path coefficients.

The application of SmartPLS in this study is supported by the findings of ([Wiguna et al., 2025](#)), who emphasize that the software significantly enhances the quality of quantitative research. SmartPLS provides methodological flexibility, strengthens the validity of constructs, and simplifies the data processing procedure, making it especially useful for analyzing complex models in social, business, and economic studies. Their work demonstrates that SmartPLS not only improves statistical accuracy but also increases researchers' confidence in interpreting results. For these reasons, the adoption of SmartPLS in this research is both methodologically justified and practically relevant.

Through this methodological framework, the study aims to produce reliable empirical findings regarding the mediating role of privacy in strengthening the usage intensity of biometric-based digital payment systems in Indonesia, particularly on the GoPay platform. Beyond its practical implications, the methodology also contributes to the academic literature by reinforcing the role of PLS-SEM as a robust analytical tool in social and economic research, as highlighted by ([Wiguna et al., 2025](#)).

Results and Discussion

This section presents the findings of the study, exploring the results of the data analysis and their implications. The discussion is based on an in-depth interpretation of these findings, with a focus on how the work contributes to the literature on digital technology adoption. The analysis was conducted using the Partial Least Squares-Structural Equation Modeling (PLS-SEM) method with the SmartPLS software.

The presentation of the results is divided into two main parts: the (1) Measurement Model Analysis (Outer Model), which assesses the validity and reliability of the research instrument, and the (2) Structural Model Analysis (Inner Model), which tests the proposed hypotheses and relationships between the variables.

Table 2. Validity and Reliability Test Results

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Convenience	0.812	0.821	0.877	0.641
Perceived Value	0.800	0.828	0.865	0.568
Privacy	0.831	0.836	0.888	0.665
Security	0.784	0.797	0.860	0.607
Trust	0.785	0.800	0.860	0.606
Usage Intensity	0.844	0.869	0.896	0.686

Source: Data Processing (2026)

As shown in Table 2, all variables have an Average Variance Extracted (AVE) value above the 0.50 threshold, which confirms their convergent validity. This indicates that the indicators accurately represent their respective latent constructs. Furthermore, the Composite Reliability and Cronbach's Alpha values for all variables were found to be above 0.70. These results demonstrate a high degree of internal consistency within the research instrument, ensuring that the data collected is reliable and suitable for analysis.

The structural model analysis reveals the relationships between the variables and the overall predictive power of the model. This section also provides a detailed discussion of the hypothesis testing results.

Table 3. Coefficient of Determination Test (R^2)

	R Square	Remarks
Privacy	0.820	82.0% of variance can be explained
Usage Intensity	0.560	56.0% of variance can be explained

Source: Data Processing, (2026)

Based on Table 3, the R^2 value for the Privacy variable is 0.820, indicating that 82.0% of the variance in user privacy perceptions can be effectively explained by the Convenience, Perceived Value, Security, and Trust variables. Additionally, the R^2 value for Usage Intensity is 0.560, suggesting that 56.0% of its variance is explained by the model. These substantial values confirm the model's high effectiveness in explaining the hypothesized relationships.

The hypothesis testing was performed to confirm the proposed relationships between the variables.

Table 4. Hypothesis Test Results

Path Relationship	P Values	Remarks
Convenience -> Privacy	0.027	Supported
Perceived Value -> Privacy	0.005	Supported
Privacy -> Usage Intensity	0.000	Supported
Security -> Privacy	0.000	Supported
Trust -> Privacy	0.807	Not Supported

Source: Data Processing (2026)

Based on Table 4, the test results provide several critical findings. First, the relationship between Convenience and Privacy is supported (P-Values = 0.027). This suggests that a higher perceived ease of use for the fingerprint feature on GoPay significantly and positively influences users' perceptions of privacy. The simplified process of not having to manually enter a PIN makes users feel more secure from threats like shoulder surfing.

Second, the hypothesis stating that Perceived Value affects Privacy is also supported (P-Values = 0.005). This result indicates that when users perceive significant benefits from the fingerprint feature, their confidence in personal data protection also increases. This is consistent with literature highlighting that perceived value can trigger a belief in data privacy.

The strongest finding of this study is the relationship between Security and Privacy, which is very significantly supported (P-Values = 0.000). This result emphatically confirms that perceived security has a dominant influence on privacy perception. When users are confident that the implemented biometric security technology is sophisticated and effective, their belief in personal data protection increases dramatically. This finding aligns with existing research that positions a sense of security as a fundamental prerequisite for trusting digital platforms.

Furthermore, the relationship between Privacy and Usage Intensity is also significantly supported (P-Values = 0.000). This is a crucial finding, proving that privacy perception is a major driver of GoPay usage intensity. When users feel their data is secure, they are more likely to use the service frequently and without hesitation.

However, a surprising result emerged from the hypothesis testing: the relationship between Trust and Privacy is not supported (P-Values = 0.807). This suggests that in the context of a digital wallet with biometric technology, general trust does not significantly influence users' privacy perceptions. This can be interpreted to mean that users prioritize more concrete and specific factors, such as security and convenience features, when forming their privacy judgments, rather than relying on a more abstract concept of trust in a brand. This novel finding provides a new perspective that in technology-dependent services, user perception is driven more by clear functional and technical aspects.

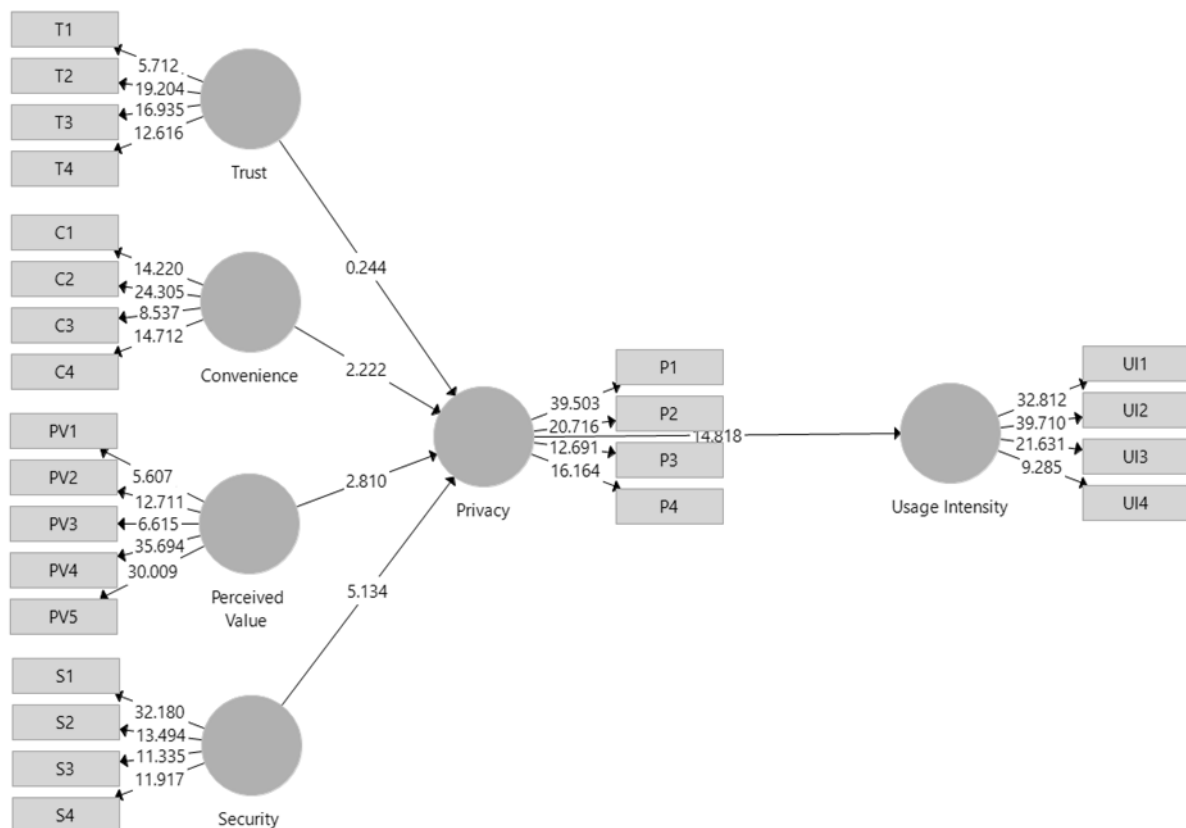


Figure 2. Final Research Model

The results of data processing in this study indicate that the variables Convenience, Perceived Value, and Security have a positive and significant effect on Privacy. This finding suggests that the ease of use, the perceived benefits, and the security aspects of the fingerprint authentication feature in GoPay significantly enhance users' perception of privacy. With a system that is easy to operate and supported by advanced biometric security, users feel that their data are safer and the application is more reliable for daily digital transactions.

The variable Privacy was also found to have a positive and significant effect on Usage Intensity. This result demonstrates that the higher the users' perception of privacy, the greater their tendency to intensively use GoPay. In other words, perceived privacy acts as a key driving factor that fosters consistent and frequent use of the application in everyday life.

On the other hand, the Trust variable did not show a significant effect on Privacy. These findings indicate that although users may generally trust the GoPay service, this trust does not always influence their perception of privacy protection. In this context, users seem to prioritize concrete aspects such as system security mechanisms, ease of use, and the tangible benefits offered by the application over the abstract concept of trust itself.

This finding differs from several previous studies that emphasized the important role of trust in shaping users' perceptions of privacy and security in digital financial services. Previous research has shown that trust is an important determining factor that influences user acceptance of biometric payment technologies and digital financial services (Liébana-Cabanillas et al., 2024; Zarco et al., 2024). Other studies have also reported that improvements in authentication systems and privacy protection mechanisms can significantly strengthen user trust in e-wallet platforms (Hassan & Shukur, 2022; Prawira et al., 2024). The inconsistency between this study and previous findings may be explained by the context of Indonesian users, who may place greater emphasis on visible technological security measures such as biometric authentication and system security features rather than relying solely on trust in service providers.

Overall, the final model highlights that Privacy plays a central mediating role in explaining the relationship between Convenience, Perceived Value, and Security with Usage Intensity. These findings underscore the importance for digital wallet providers to emphasize advanced security technologies, user-friendly features, and clear functional benefits. These factors have been proven to shape a stronger perception of privacy, which in turn significantly increases the adoption and continued use of GoPay.

Conclusion

This study identifies key factors that influence the intensity of biometric-based digital wallet usage, particularly GoPay. The findings show that convenience, perceived value, and security have a positive and significant influence on privacy, while privacy significantly increases usage intensity. However, trust does not have a significant influence on the perception of privacy, indicating that users tend to consider concrete technological aspects such as security and system functionality when evaluating privacy in biometric payment systems.

The theoretical contribution of this study lies in confirming the mediating role of privacy in the relationship between convenience, perceived value, security, and usage intensity. By integrating TAM, UTAUT2, and Privacy Calculus Theory, this study enriches the fintech adoption literature by showing that privacy perceptions are an important mechanism linking technological factors to user behavior.

Practically, digital wallet providers need to prioritize strengthening privacy protection through more robust security systems, transparent data governance, and user-friendly application design. These efforts can increase user trust and encourage more consistent use of biometric-based digital payment services.

References

- Abdul-Halim, N. A., Vafaei-Zadeh, A., Hanifah, H., Teoh, A. P., & Nawaser, K. (2022). Understanding the determinants of e-wallet continuance usage intention in Malaysia. *Quality and Quantity*, 56(5), 3413–3439. <https://doi.org/10.1007/s11135-021-01276-7>.
- Auliano, A. B., Dongoran, F. L., Ferdiansyah, M. D., Darusman, R., & Fitriansyah, S. (2025). Strategi Manajemen Sekuriti Untuk Meningkatkan Kepercayaan Pengguna Terhadap Transaksi E-Wallet. *Journal of Informatic and Information Security*, 5(2), 201–212. <https://doi.org/10.31599/3p9mf764>.
- Faridah, N. Z., Kuswati, R. (2024). Peran Kepercayaan Sebagai Pemediasi Pengaruh Kegunaan, Keamanan,

- Kemudahan Terhadap Adopsi E-Wallet. *Jurnal Ilmiah Manajemen Dan Bisnis*, 55–77. [10.30606/f90p2n87](https://doi.org/10.30606/f90p2n87).
- Franque, F. B., Oliveira, T., & Tam, C. (2021). Understanding the factors of mobile payment continuance intention: empirical test in an African context. *Heliyon*, 7(8), e07807. <https://doi.org/10.1016/j.heliyon.2021.e07807>.
- Hanifah, P. R., Rachbini, W., Transaksi, K., Rekomendasi, N., & Pengguna, L. (2025). Peran Keamanan dan Kualitas Prduk dalam meningkatkan Niat Rekomendasi Pada Pengguna dompet Digital. *Neraca Manajemen, Ekonomi*, 19(10) <https://cibangsa.com/index.php/musyari/article/view/2679>.
- Hassan, M. A., & Shukur, Z. (2022). Device identity-based user authentication on electronic payment system for secure e-wallet apps. *Electronics (Switzerland)*, 11(1). <https://doi.org/10.3390/electronics11010004>.
- Ismail, T., Sugiono, A., & Subagja, G. (2023). Analisis Penerimaan Pengguna Produk E-Money Gopay Terhadap Minat Menggunakan Go-Pay Di Bandar Lampung. *Jurnal Kompetitif Bisnis*, 1(Vol 1 No 12 (2023): Jurnal Kompetitif Bisnis), 8–11. <https://jkb.fisip.unila.ac.id/index.php/jkb/article/view/232/148>.
- Jannah, M., Hidayat, M. F., Agustiyani, M., Buana, P. W., & Purwani, F. (2024). Implementasi Autentikasi Biometrik Untuk Meningkatkan Keamanan Dan Privasi Pengguna Dompet Digital. *Journal of Scientech Research and Development*, 6(2), 531–539. <https://doi.org/10.56670/jsrd.v6i2.606>.
- Kajol, K., Singh, R., & Paul, J. (2022). Adoption of digital financial transactions: A review of literature and future research agenda. *Technological Forecasting and Social Change*, 184(August), 121991. <https://doi.org/10.1016/j.techfore.2022.121991>.
- Khoiriah, S., Salsabila, A., Camberra, D. D., Syafri, E., Layyin, H. L., Fathurrahman, R., & Marjohan, M. (2025). Keamanan dan Privasi dalam Keuangan Digital. *Jurnal Publikasi Sistem Informasi Dan Manajemen Bisnis*, 4(2), 409–418. <https://doi.org/10.55606/jupsim.v4i2.4524>.
- Kusuma, K. N., Purwinarti, T., & Mariam, I. (2021). Pengaruh Perceived Ease Of Use Dan Perceived Security Terhadap Minat Menggunakan Gopay. *Seminar Nasional Riset Terapan Administrasi Bisnis Dan MICE*, 10(1), 358–368.
- Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F., & Higuera-Castillo, E. (2024). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information and Management*, 61(2). <https://doi.org/10.1016/j.im.2023.103907>.
- Marakalala, M. C. (2023). Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud. *OIDA International Journal of Sustainable Development*, 16(5), 19–30.
- Mulyana, S. L. (2025). Implementasi Cyber Security Dalam Sistem. *Jurnal Ilmiah Ekonomi Manajemen Bisnis Dan Akuntansi*, 2(4), 276–289.
- Mulyawan, S. K. Z., & Sharif, O. O. (2022). Analisis Customer Value Index dalam Menggunakan Mobile Payment di DKI Jakarta. *Jurnal Nusantara Aplikasi Manajemen Bisnis*, 7(1), 54–72. <https://doi.org/10.29407/nusamba.v7i1.16179>.
- Pattnaik, D., Ray, S., & Raman, R. (2024). Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review. *Heliyon*, 10(1), e23492. <https://doi.org/10.1016/j.heliyon.2023.e23492>.
- Prawira, F. R., Prakoso, N. T., Handayani, P. W., & Harahap, N. C. (2024). The influence of information security factors on the continuance use of electronic wallet. *Procedia Computer Science*, 234(2023), 1467–1475. <https://doi.org/10.1016/j.procs.2024.03.147>.
- Putri, P. A., Prasetyo, S. A., & Ageng, A. S. R. (2024). Analisis Pengaruh Keamanan Dan Kemudahan Dalam Penggunaan E-Wallet Gopay. *Senatib*, 531–536.
- Rhois, M. N. M., Rachmadi, A., & Wijoyo, S. H. (2024). Analisis Faktor yang Memengaruhi Perilaku Penggunaan Aplikasi GoPay: Transfer & Payment Mempengaruhi Model Unified Theory Of Acceptance And Use Of Technology (UTAUT). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 8(8), 1–13.
- Sahabuddin, R., Azhari, A., Manggarani, S., Ramadhani, F. A., Astuty, L. M., & Purnama, A. (2025). Pengaruh Kemudahan, Keamanan, Promosi, Dan Kepercayaan Penggunaan Dompet Digital Di Kalangan Masyarakat. *Jurnal Rumpun Manajemen Dan Ekonomi*, 2(3), 409–420. <https://ejurnal.kampusakademik.co.id/index.php/jrme/article/view/4536>.
- Saputri, V. D. (2023). Implementation Of Biometric-Based Security System On Mobile Banking Application. *Jurnal Komputer Indonesia*, 2(1), 25–32. <https://doi.org/10.37676/jki.v2i1.565>.

- Sasongko, D. T., Handayani, P. W., & Satria, R. (2021). Analysis of factors affecting continuance use intention of the electronic money application in Indonesia. *Procedia Computer Science*, 197(2021), 42–50. <https://doi.org/10.1016/j.procs.2021.12.116>.
- Secinaro, S., Lanzalonga, F., Oppioli, M., & de Nuccio, E. (2025). The effects of disruptive technologies on accountability in fintech industry: Using bibliometric analysis to develop a research agenda. *Research in International Business and Finance*, 76(May 2023). <https://doi.org/10.1016/j.ribaf.2025.102816>.
- Sethi, M., Bohra, N. S., Johri, A., & Asif, M. (2025). Emerging dimensions in Fintech: Insights from bibliometric analysis. *Digital Business*, 5(1). <https://doi.org/10.1016/j.digbus.2025.100113>.
- Simanjuntak, I. G., Saputra, M. H., Melisa, Manurung, I. S., Cristhian, I., & Lim, V. (2024). Analisa Pengaruh Kemudahan, Kepercayaan dan Keamanan terhadap Kepuasan Pengguna Aplikasi Dana. *Ekraf: Jurnal Ekonomi Kreatif Dan Inovatif Indonesia*, 1(2), 102–113. <https://doi.org/10.59965/ekraf.v1i2.60>.
- Wang, K.-H. (2025). Beyond digital finance: The impact of internet banking adoption on subjective life satisfaction. *Finance Research Open*, 1(2), 100012. <https://doi.org/10.1016/j.finr.2025.100012>.
- Widiyanto, M. (2024). Implementasi Fingerprint Dan Algoritma Riverst Shamir Adleman Untuk Kemanan Data. *Jurasik (Jurnal Riset Sistem Informasi ...)*, 9, 847–855. <http://ejurnal.tunasbangsa.ac.id/index.php/jurasik/article/view/816%0Ahttp://ejurnal.tunasbangsa.ac.id/index.php/jurasik/article/download/816/790>.
- Widyaretno, N., & Indriyanti, A. D. (2023). Analisis Penerimaan Pengguna terhadap Penerapan Biometric Authentication pada Shopee-Pay menggunakan Metode UTAUT. *Journal of Emerging Information Systems and Business Intelligence*, 4(04), 17–25. <https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/56007>.
- Wiguna, I. N. A., Zebua, D., Lopez, V. M. D., Nastiti D. W., Daud, C. T. P., & Sihombing, M. I. (2025). Pelatihan Penggunaan Aplikasi Smart Pls Sebagai Alat Pengolahan Data Penelitian Mahasiswa. *Jurnal Abdimas Sosek (Jurnal Pengabdian dan Pemberdayaan Masyarakat)*, 5(1), 1–4.
- Zarco, C., Giráldez-Cru, J., Cordon, O., & Liébana-Cabanillas, F. (2024). A comprehensive view of biometric payment in retailing: A complete study from user to expert. *Journal of Retailing and Consumer Services*, 79(February 2024). <https://doi.org/10.1016/j.jretconser.2024.103789>.