International Journal Software Engineering and Computer Science (IJSECS)
5 (2), 2025, 781-791
Published Online August 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i2.4518.

RESEARCH ARTICLE Open Access

User Trust, Security, and Data Privacy Awareness in GoPay Usage Using Protection Motivation Theory (PMT)

Diva Ayu Gitareswara *
Information Systems Study Program, Faculty of Science and Technology, Universitas Jambi, Muaro Jambi Regency, Jambi Province, Indonesia.
Corresponding Email: gitareswarad@gmail.com.

Tri Suratno
Information Systems Study Program, Faculty of Science and Technology, Universitas Jambi, Muaro Jambi Regency, Jambi Province, Indonesia.

Dewi Lestari
Information Systems Study Program, Faculty of Science and Technology, Universitas Jambi, Muaro Jambi Regency, Jambi Province, Indonesia.

Received: June 13, 2025; Accepted: July 20, 2025; Published: August 1, 2025.

Abstract: The widespread adoption of GoPay in Indonesia has raised significant questions about user data privacy and security, dimensions frequently overlooked by traditional utility-focused adoption models such as TAM and UTAUT. This research addresses that gap by applying Protection Motivation Theory (PMT) to examine the psychological drivers behind GoPay usage intention. Through a quantitative national survey of 105 active users analyzed via PLS-SEM, the model explained 69.3% of variance in behavioral intention (R^2=0.693). Results show that privacy concern, perceived severity, perceived vulnerability, response cost, response efficacy, and trust significantly and positively influence usage intention. In contrast, security features and user self-efficacy were not significant drivers. The findings demonstrate that users' behavioral intentions are more strongly influenced by their evaluation of potential threats and confidence in the service provider's protective capabilities rather than technical security features or personal competence alone. The study advances understanding of digital payment adoption by revealing that psychological threat assessment processes, rather than technical security perceptions, primarily drive user decisions. GoPay users prioritize the platform's ability to protect them over their own technical skills or general security features. These findings offer practical implications for digital wallet providers seeking to enhance user adoption through targeted trust-building strategies rather than solely focusing on technical security improvements.

Keywords: GoPay; Protection Motivation Theory; Behavioral Intention.

1. Introduction

Financial technology advancement has fundamentally transformed business models from conventional to digital platforms, enabling efficient remote transactions [3]. Indonesia, recognized as one of the world's leading e-commerce adoption countries, has witnessed digital wallets becoming integral to citizens' transaction activities [9]. GoPay, as a major player, reportedly serves tens of millions of active users, underlining its systemic role in the national digital payment ecosystem. According to Bank Indonesia's 2023 payment system statistics, digital wallet transactions reached 7.8 billion with a total value of Rp 28.8 trillion, demonstrating the massive scale of adoption across the archipelago.

While several studies have examined GoPay's functional aspects and usability across various services [1], a substantial literature gap remains regarding how psychological factors drive users to adopt or neglect data protection measures. Many researchers focus on transactional benefits, while users' protective motivations are often overlooked. To bridge the understanding gap, Protection Motivation Theory (PMT) provides a relevant and tested framework for understanding how individuals respond to threats based on risk evaluation (threat appraisal) and available protection mechanism effectiveness (coping appraisal) [13]. The rapid digitization of financial services in Indonesia has created a unique behavioral landscape where users must balance convenience with security concerns. Unlike traditional banking systems where physical presence provides psychological comfort, digital wallets operate entirely in virtual spaces, creating new forms of vulnerability perception.

The Indonesian market, characterized by diverse digital literacy levels and varying socioeconomic backgrounds, presents a particularly interesting case study for understanding protection motivation dynamics. Recent cybersecurity incidents in the Indonesian financial technology sector have heightened public awareness about digital payment risks. High-profile data breaches and fraudulent activities have created a climate where users are increasingly conscious of potential threats. The heightened awareness creates an opportunity to examine how threat perceptions influence behavioral intentions in real-world conditions rather than hypothetical scenarios. The interplay between media coverage of security incidents and individual risk assessment processes adds another layer of complexity to user decision-making.

However, the popularity accompanies concerns regarding data security and privacy [10][11]. User trust becomes a fundamental factor, heavily influenced by their perceptions of security and privacy protection offered [2][12]. Several studies have examined GoPay adoption from functional perspectives such as ease of use and benefits (e.g., through TAM/UTAUT models) [1][17]. Nevertheless, a literature gap persists in understanding how users' protective motivations—their psychological responses to cyber threats—shape usage intentions. Many researchers tend to focus on transactional benefits, while users' cognitive mechanisms in evaluating threats and their ability to protect themselves are often neglected.

Furthermore, the Indonesian regulatory environment has evolved significantly with the implementation of Personal Data Protection Law (UU PDP) in 2022, creating new expectations for data handling practices. Users are now more aware of their rights regarding personal information, potentially altering their evaluation criteria for digital payment services. The regulatory shift provides a unique temporal framework for examining how changing legal frameworks influence user perceptions and behavioral intentions. The research addresses several critical questions: Do users with higher threat awareness actually exhibit stronger usage intentions due to their proactive risk management approach? How do individual differences in digital literacy affect the relationship between perceived threats and behavioral responses? What role does social influence play in shaping threat perceptions and coping strategies? These questions are particularly relevant in the Indonesian setting, where collective decision-making and social proof often influence individual choices. Therefore, the research formulates the main problem: How do user trust, security perceptions, and data privacy awareness, when analyzed through the Protection Motivation Theory lens, influence behavioral intention to use GoPay in Indonesia? The study will specifically investigate the dynamics between threat perceptions (severity and vulnerability), self-protection capability evaluation (response efficacy and self-efficacy), and trust's crucial role in shaping users' final decisions to continue using GoPay services amid existing cyber risk potential.

Based on the background above, the research formulates the main problem: How do threat evaluation (severity and vulnerability), coping evaluation (response efficacy, self-efficacy, and response cost), and external variables such as trust and security simultaneously influence behavioral intention to use GoPay in Indonesia within the Protection Motivation Theory framework? The research problem can be further broken down into specific sub-questions: Which threat appraisal factors (perceived severity vs. perceived vulnerability) have stronger predictive power for behavioral intention? How do coping appraisal mechanisms interact with external trust factors in determining usage decisions? What mediating effects exist between demographic characteristics and PMT constructs? How do cultural factors specific to Indonesian society influence the traditional PMT model?

Research objectives are: First, empirically test the GoPay usage behavioral intention model adapted from the PMT framework. The testing involves validating the theoretical model in the Indonesian digital payment

setting and assessing the adequacy of PMT constructs in explaining user behavior patterns. The testing will employ advanced statistical techniques to ensure robust model validation and cross-validation procedures to confirm generalizability. Second, identify the most dominant factors from threat and coping evaluation processes that shape user decisions. Through comparative analysis of effect sizes and path coefficients, the research will determine which psychological mechanisms exert the strongest influence on behavioral intentions. The identification will help prioritize intervention strategies and resource allocation for service providers. Third, provide practical recommendations for digital wallet service providers to build trust and encourage safe usage. Based on empirical findings, the research will develop actionable strategies that address the most influential psychological drivers identified in the study. These recommendations will be tailored to the Indonesian market characteristics and regulatory environment. The research significance extends beyond academic advancement to practical implications for industry stakeholders, policymakers, and users themselves. For industry practitioners, the findings will inform user experience design, security communication strategies, and customer retention programs. Policymakers can leverage the insights to develop more effective consumer protection frameworks and digital literacy initiatives. Users will benefit from improved service designs that better address their psychological needs and security concerns.

2. Related Work

2.1 Literature Review on GoPay Usage Studies

Previous research on GoPay usage reveals both consistent patterns and contradictory findings across different studies. Trust consistently emerges as a fundamental factor significantly affecting GoPay loyalty, satisfaction, and usage intention, functioning both as an independent variable and mediator [9][12]. Similarly, perceived ease of use generally appears as a primary adoption driver, becoming the most dominant factor for certain demographics such as Generation X users [11][17]. However, clear discrepancies exist regarding security and privacy variables. Some studies conclude that security and privacy positively influence usage [19], while other research finds that both factors, along with perceived risk, do not significantly affect GoPay usage decisions or intentions [17]. The contradictory findings regarding security and privacy suggest that while trust and ease of use serve as main pillars in the GoPay ecosystem, security and privacy roles remain inconsistent across different research contexts. These variations likely stem from differences in research methodology, demographic samples, and temporal factors. For instance, studies conducted before major cybersecurity incidents may yield different results compared to those conducted afterward, as public awareness and concern levels fluctuate based on recent events. Jamiah, Purwanto, and Asmike (2022) found that trust mediates the relationship between perceived ease of use and security on usage intention in Madiun City [9]. Their study reinforced the central role of trust while simultaneously showing security's indirect rather than direct influence. Conversely, Kamil (2019) demonstrated that trust, security, and perceived ease of use all directly influence GoPay usage intention [10]. The difference in findings between these studies may be attributed to geographical variations, sample characteristics, or measurement approaches.

Liani and Yusuf (2021) examined the relationship between e-trust, e-satisfaction, and e-loyalty among GoPay users, finding that trust significantly influences loyalty through satisfaction mediation [12]. Their work established trust as not merely a usage predictor but also a retention factor. Meanwhile, Sukmawati and Kowanda (2022) focused on security, perceived ease, and perceived benefits, concluding that all three factors positively influence usage decisions [17]. However, their study did not include privacy concerns or risk perceptions, potentially limiting the scope of security-related findings. The role of perceived risk presents another area of inconsistency. Prasetyo and Wardhani (2022) found that perceived risk and trust both influence behavioral intention, with trust having a stronger effect [15]. Their study suggested that users can simultaneously hold concerns about risks while maintaining usage intentions, provided trust levels remain high. This finding challenges traditional risk-avoidance models and supports the Protection Motivation Theory approach, where threat awareness can coexist with continued usage behavior.

2.2 Protection Motivation Theory in Digital Payment

Protection Motivation Theory has been applied in various technology adoption contexts, but its application to digital payment systems remains limited. Marikyan and Papagiannidis (2023) provide a recent review of PMT applications, noting its effectiveness in explaining user behavior when threats and protective responses are clearly identifiable [13]. The theory's dual-process model, involving threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy, self-efficacy, and response cost), offers a more nuanced understanding of user decision-making compared to traditional adoption models. In the digital payment domain, threat appraisal involves users' evaluation of potential financial losses, privacy breaches, and identity theft risks. Coping appraisal encompasses their assessment of available protective measures, personal capabilities to implement these measures, and associated costs. The theory's strength lies in

recognizing that users can simultaneously acknowledge threats while continuing usage if they believe effective protection mechanisms exist.

2.3 Trust and Security in Digital Financial Services

Trust research in digital financial services has evolved from simple binary constructs to multidimensional frameworks. Delima Sari (2023) discusses privacy and data security challenges in digital services, emphasizing the growing importance of individual data protection [2]. The study highlights how regulatory changes, such as Indonesia's Personal Data Protection Law, influence user expectations and trust formation processes. Security perceptions in digital payments involve both technical and psychological dimensions. Technical security refers to encryption, authentication protocols, and fraud detection systems, while psychological security relates to users' confidence in these systems' effectiveness. Gatot Efrianto and Nia Tresnawaty (2021) found that privacy, security, trust, and experience all influence fintech usage, but their relative importance varies across user segments [5].

2.4 Research Gaps and Hypothesis Development

The literature review reveals several gaps that this research addresses. First, most existing studies apply traditional adoption models (TAM, UTAUT) that focus on utility and ease of use while neglecting psychological responses to threats. Second, the contradictory findings regarding security and privacy effects suggest the need for a more sophisticated theoretical framework that can explain these variations. Third, limited research has examined how threat perceptions and coping mechanisms interact in the Indonesian digital payment context. Based on Protection Motivation Theory and the literature review, the following hypotheses are formulated:

H1 : Perceived severity of risks when using GoPay positively influences behavioral intention to use GoPay. Users who recognize the serious consequences of potential security breaches are more likely to engage with the service because they value the protective measures offered.

H2 : Perceived vulnerability to security and privacy risks when using GoPay positively influences behavioral intention to use GoPay. Users who acknowledge their susceptibility to threats are motivated to use services that provide adequate protection.

H3 : Response efficacy of GoPay in managing security and data privacy positively influences behavioral intention to use GoPay. Users who believe GoPay effectively protects against identified threats are more likely to continue usage.

H4 : Self-efficacy in using GoPay safely positively influences behavioral intention to use GoPay. Users who feel confident in their ability to protect themselves while using the service show stronger usage intentions.

H5 : Response cost for using GoPay safely positively influences behavioral intention to use GoPay. When users perceive that the effort required to use GoPay securely is reasonable, they are more likely to maintain usage intentions

H6 : Privacy concern when using GoPay positively influences behavioral intention to use GoPay. Paradoxically, users with higher privacy awareness may show stronger intentions to use services they trust to handle their data appropriately.

H7 : Trust in GoPay positively influences behavioral intention to use GoPay. Users who trust the service provider are more likely to continue usage despite potential risks.

H8 : Perceived security level in GoPay usage positively influences behavioral intention to use GoPay. Users who perceive high security standards are more inclined to maintain their usage intentions.

3. Research Method

3.1 Population and Sample

This research employs a quantitative approach with an explanatory research design that aims to test and explain causal relationships between variables. The population in this study consists of all GoPay application users in Indonesia. Sample selection was conducted using purposive sampling technique, which is a sample selection method based on specific considerations and criteria established by researchers to ensure relevance to research objectives [16]. The main criterion for respondents is active users who have conducted transactions using GoPay at least three times. The sample size was set at 105 respondents, which is considered representative and meets the guidelines from Hair (2013) who recommends a sample size between 5 to 10 times the number of research indicators [8]. The purposive sampling approach was chosen to ensure data quality and relevance to the research context. Active users with multiple transaction experiences are more

likely to have formed stable perceptions about GoPay's security, privacy, and trust aspects. The minimum three-transaction criterion ensures that respondents have sufficient exposure to the platform's features and potential risks, enabling them to provide informed responses about their behavioral intentions and protection motivations.

3.2 Research Variables

Primary data collection was conducted through online questionnaire distribution using the Google Forms platform. The research instrument employs a 4-point Likert scale (Strongly Agree, Agree, Disagree, Strongly Disagree) to measure all statement items. The selection of a 4-point scale was intentionally made to eliminate neutral response options, aiming to encourage respondents to provide more definitive attitudes, thereby producing more actionable data, consistent with recommendations from previous research (Nowlis et al., 2002; Garland, 1991). The independent variables (exogenous) in this research are Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, Privacy Concern, Trust, and Security. Meanwhile, the dependent variable (endogenous) being tested is Behavioral Intention. Each variable was operationalized through multiple indicators adapted from established scales in previous literature, with modifications to suit the GoPay usage context in Indonesia. Perceived Severity measures users' evaluation of the seriousness of potential consequences from security breaches or privacy violations. Perceived Vulnerability assesses users' beliefs about their susceptibility to such threats. Response Efficacy evaluates users' perceptions of GoPay's effectiveness in protecting against identified threats. Self-Efficacy measures users' confidence in their own ability to use GoPay safely. Privacy Concern captures users' worries about personal data handling. Trust reflects users' confidence in GoPay as a service provider. Security measures users' perceptions of the platform's security features and capabilities.

3.3 Data Analysis Method

The data analysis technique used is Structural Equation Modeling (SEM) with a Partial Least Squares (PLS) approach, operated through SmartPLS software. Data analysis was conducted in two main stages. The first stage is the evaluation of the measurement model (outer model) to ensure research instruments are valid and reliable. Convergent validity is tested through loading factor values (> 0.5), discriminant validity through Average Variance Extracted (AVE) values, while reliability is tested through Composite Reliability and Cronbach's Alpha values (> 0.7). The second stage is the evaluation of the structural model (inner model) to test relationships between constructs, assessed through R-Square values. Finally, hypothesis testing is conducted using bootstrapping procedures to obtain T-statistic values. According to general guidelines [7], a hypothesis is declared to have significant influence if it has a T-statistic value > 1.96 or p-value < 0.05. The choice of PLS-SEM over covariance-based SEM (CB-SEM) was made considering several factors. First, PLS-SEM is more suitable for exploratory research and theory development, which aligns with this study's objective of applying PMT in the Indonesian digital payment context. Second, PLS-SEM performs better with smaller sample sizes, making it appropriate for the 105-respondent sample. Third, PLS-SEM is less restrictive regarding data distribution assumptions, providing more flexibility in analysis. Fourth, the method is particularly effective for complex models with multiple constructs and indicators, which characterizes this research model.

4. Result and Discussion

4.1 Results

4.1.1 Data Collection Stage

The data collection stage in this research was conducted by distributing online questionnaires to respondents in the form of surveys to GoPay application users in Indonesia. The questionnaire used in this research required a minimum of 105 questionnaires based on the sample and population determination using Hair's formula, so a total of 105 questionnaires would be used for processing and analysis.

Table 1. Questionnaire Collection Results

Description	Number
Questionnaires received	179
Questionnaires not meeting requirements	74
Questionnaires meeting requirements	105

Based on the data in the table, it can be concluded that the total questionnaires received were 179, with 74 questionnaires not meeting the requirements. Since this research had predetermined the sample size as 105 questionnaires, the excess responses were filtered based on completion criteria and response quality.

4.1.2 Measurement Model Test Results (Outer Model)

The measurement model, known as the outer model in PLS-SEM methodology, functions to model the relationship between variables and their forming indicators. The quality of this measurement model is assessed through a two-stage evaluation procedure. The first stage is validity testing, divided into convergent validity and discriminant validity to ensure that each indicator measures the appropriate construct. The second stage is reliability testing measured by composite reliability to assess the internal consistency of indicators. The calculation of these metrics was performed based on the PLS Algorithm using SmartPLS software. To ensure instrument validity, convergent validity testing was conducted. This evaluation was performed by examining whether the loading factor values of each indicator and the Average Variance Extracted (AVE) values of each construct met the recommended thresholds. According to [6], an indicator is declared valid if its loading factor value exceeds 0.70 (with tolerance in the 0.50-0.60 range). Additionally, validity at the construct level is achieved if the AVE value is greater than 0.50. The calculation of these values was performed through iterative procedures until convergence using PLS-SEM software. Table 2 below presents the detailed results of this testing.

Table 2. Convergent Validity Test Results

Variable	Indicator	Outer Loading	Status	AVE
Perceived Vulnerability	PV1	0.844	Valid	0.722
	PV2	0.853	Valid	
	PV3	0.852	Valid	
Perceived Severity	PS1	0.898	Valid	0.799
	PS2	0.889	Valid	
Response Efficacy	RE1	0.870	Valid	0.698
	RE2	0.821	Valid	
	RE3	0.814	Valid	
Self-Efficacy	SE1	0.917	Valid	0.855
	SE2	0.932	Valid	
Response Cost	RC1	0.926	Valid	0.811
	RC2	0.899	Valid	
	RC3	0.876	Valid	
Privacy Concern	PC1	0.932	Valid	0.879
	PC2	0.943	Valid	
Trust	T1	0.937	Valid	0.868
	T2	0.926	Valid	
Security	SC1	0.853	Valid	0.772
	SC2	0.904	Valid	
Behavioral Intention	BI1	0.921	Valid	0.855
	BI2	0.928	Valid	

From the data results in the table above, all indicators have outer loading values > 0.7. Therefore, it can be concluded that all indicators in this research have good and acceptable convergent validity levels. The next outer model testing is discriminant validity evaluation, which in this research refers to cross-loading criteria. According to this approach, discriminant validity is fulfilled if each indicator shows the highest loading value on the latent construct it measures, not on other constructs. If all indicators in the model meet this standard, it can be concluded that each construct has clear differences from one another [6]. The detailed cross-loading values from this analysis are displayed in Table 3.

Table 3. Cross Loading

Code	BI	PC	PS	PV	RC	RE	SC	SE	T
BI1	0.921	0.503	0.338	0.469	0.566	0.301	0.302	0.409	0.560
BI2	0.928	0.604	0.284	0.425	0.551	0.318	0.462	0.423	0.585
PC1	0.538	0.932	0.091	0.272	0.347	0.180	0.383	0.196	0.373
PC2	0.585	0.943	0.142	0.339	0.348	0.174	0.298	0.295	0.457
PS1	0.306	0.070	0.898	0.042	0.157	-0.056	0.119	0.167	0.319
PS2	0.294	0.156	0.889	0.048	0.117	-0.019	0.204	0.078	0.288
PV1	0.432	0.352	0.023	0.844	0.265	0.128	0.179	0.239	0.379
PV2	0.391	0.195	0.008	0.853	0.326	0.080	0.061	0.135	0.255
PV3	0.406	0.279	0.097	0.852	0.286	0.101	0.219	0.214	0.318
RC1	0.575	0.308	0.131	0.305	0.926	0.216	0.300	0.343	0.442
RC2	0.558	0.403	0.130	0.349	0.899	0.314	0.266	0.258	0.491

RC3	0.493	0.289	0.157	0.269	0.876	0.132	0.230	0.245	0.336
RE1	0.320	0.146	0.024	0.177	0.228	0.870	0.057	0.264	0.151
RE2	0.284	0.144	-0.097	0.086	0.219	0.821	0.283	0.329	0.102
RE3	0.220	0.193	-0.042	0.014	0.167	0.814	0.055	0.188	0.112
SC1	0.326	0.294	0.132	0.123	0.209	0.103	0.853	0.166	0.181
SC2	0.398	0.338	0.179	0.190	0.303	0.173	0.904	0.266	0.253
SE1	0.395	0.227	0.114	0.202	0.280	0.369	0.242	0.917	0.263
SE2	0.436	0.259	0.139	0.227	0.301	0.225	0.224	0.932	0.272
T1	0.599	0.402	0.314	0.330	0.446	0.154	0.237	0.242	0.937
T2	0.554	0.428	0.320	0.373	0.436	0.120	0.229	0.300	0.926

Table 3 presents the cross-loading test results that confirm the model's discriminant validity. It is evident that each indicator has a higher loading value on its parent construct and exceeds 0.7, while its loading values to other constructs are lower. This condition indicates that discriminant validity criteria have been satisfactorily met, confirming that each variable in this research represents distinct constructs. Reliability assessment in this research uses composite reliability and Cronbach's alpha metrics to ensure measurement tool consistency. The criteria for determining fulfilled reliability is if the values for both metrics are greater than 0.70 [6]. Table 4 below displays the calculation results of both values as the basis for model reliability evaluation.

Table 4. Reliability Test

Variable	Composite Reliability	Status
Perceived Vulnerability	0.886	Valid and reliable
Perceived Severity	0.888	Valid and reliable
Response Efficacy	0.874	Valid and reliable
Self-Efficacy	0.922	Valid and reliable
Response Cost	0.928	Valid and reliable
Privacy Concern	0.936	Valid and reliable
Trust	0.930	Valid and reliable
Security	0.871	Valid and reliable
Behavioral Intention	0.922	Valid and reliable

Based on the data in Table 4, both Composite Reliability and Cronbach's alpha values for all constructs show figures above 0.70. Therefore, it can be concluded that all constructs have good reliability. Thus, the next testing stage, namely structural model testing (inner model), can be conducted.

4.1.3 Structural Model Test Results (Inner Model)

The second stage of analysis using PLS-SEM is the structural model test (inner model). This structural model is conducted as testing between research constructs, namely relationships between latent variables and other latent variables. This structural model is conducted through several testing stages, consisting of R-Square testing (Coefficient of determination), F-Square (f2 effect size), and Q-Square (predictive relevance). R-Square is used to measure how much influence independent variables have on dependent variables. According to Ghozali & Latan (2020) [6], an R-Square value of 0.75 indicates that the model is categorized as strong, 0.50 indicates that the model is categorized as moderate, and 0.25 indicates that the model is categorized as weak. The R-Square value results can be seen in Table 5.

Table 5. R-Square Test

Variable	R Square	Status
BI	0.693	Moderate

The inner model evaluation in Table 5 reveals that the research model has moderate predictive strength for the Behavioral Intention variable. This conclusion is based on the R-Square (R^2) value of 0.693, meaning that all independent variables together can explain 69.3% of the variation in Behavioral Intention. This classification of model strength as 'Moderate' aligns with commonly used guidelines in PLS-SEM analysis. To determine the strength of influence of each predictor variable on the structural model, f-Square (f2) analysis was conducted. This method quantifies the significance of a variable's impact on the dependent variable it influences. According to Ghozali & Latan (2020) [6], f2 value interpretation is categorized into three levels: small (0.02), medium (0.15), and large (0.35), with values below 0.02 considered to have no effect. The f2 calculation results data in this research are summarized in Table 6.

Table 6. F-Square Test

	BI	PC	PS	PV	RC	RE	SC	SE	T
BI									
PC	0.151								
PS	0.075								
PV	0.080								
RC	0.118								
RE	0.048								
SC	0.022								
SE	0.040								
T	0.074								

The data in the table above presents f-Square (f2) values that measure the magnitude of influence of each exogenous variable on Behavioral Intention. Analysis results show that Privacy Concern has the strongest effect size (f2=0.151), which can be classified as medium influence. Other variables show small influence, including Response Cost (f2=0.118), Perceived Vulnerability (f2=0.080), Perceived Severity (f2=0.075), Trust (f2=0.074), Response Efficacy (f2=0.048), Self-Efficacy (f2=0.040), and Security (f2=0.022). To validate the model's predictive capability, Q-Square (Q2) testing was conducted. This metric, also known as predictive relevance, assesses model accuracy based on its ability to reproduce observed values. Using the blindfolding procedure [6], a model is considered to have good predictive relevance if it produces Q2>0 values. The Q2 values obtained from the analysis are presented in the table below.

Table 7. Q-Square Test

Variable	Q-Square	Predictive Relevance
Behavioral Intention	0.553	Yes

Based on the data processing results in the table above, it shows that the Behavioral Intention variable has a Q-Square value greater than zero, namely 0.553, so it can be concluded that the model has predictive relevance.

4.1.4 Hypothesis Testing Results

To test research hypotheses, significance analysis was used through t-statistic values generated from the bootstrapping procedure. The decision criteria for this testing are based on a two-tailed test with a 95% confidence level (α=0.05). According to guidelines from Ghozali & Latan (2020) [6], a hypothesis is declared statistically significant if the obtained t-statistic value is higher than 1.96. Based on these criteria, the analysis results conclude that 6 out of eight hypotheses are accepted, as detailed in Table 8.

Table 8. Hypothesis Testing Results

Hypothesis	T Statistics	P-Values	Status
H1: PC -> BI	3.415	0.001	Accepted
H2: PS -> BI	2.717	0.007	Accepted
H3: PV -> BI	2.582	0.010	Accepted
H4: RC -> BI	3.772	0.000	Accepted
H5: RE -> BI	2.517	0.012	Accepted
H6: SC -> BI	1.268	0.205	Rejected
H7: SE -> BI	1.690	0.091	Rejected
H8: T -> BI	2.678	0.007	Accepted

The table above presents hypothesis testing results obtained through the bootstrapping method. The decision to accept or reject hypotheses is based on two-tailed test criteria with a 5% significance level (α=0.05). A hypothesis is considered significant and accepted if the T-Statistic value is greater than 1.96 and the P-Values are less than 0.05. Based on these criteria, analysis results show that out of eight proposed hypotheses, six hypotheses are accepted and two hypotheses are rejected.

4.2 Discussion

The acceptance of hypotheses H1, H2, H3, and H5 validates core PMT principles within the GoPay usage framework. Perceived Severity (H1) and Perceived Vulnerability (H2) demonstrate significant influence, indicating that users actively engage in threat evaluation processes. When individuals recognize serious potential consequences and acknowledge their susceptibility to risks, these perceptions actually strengthen their usage intentions rather than diminish them. Response Efficacy (H3) and Response Cost (H5) similarly

show strong effects, revealing that users become more motivated when they believe GoPay effectively protects them and when they consider security measures reasonably manageable. Privacy Concern emerges as the strongest predictor with an effect size of 0.151, creating a fascinating paradox in user behavior. Instead of discouraging platform usage, heightened privacy awareness actually reinforces behavioral intentions. Users who demonstrate greater privacy consciousness appear more discerning in their service selection, gravitating toward platforms they perceive as trustworthy data handlers. GoPay seems to satisfy these elevated expectations, transforming potential concerns into confidence drivers. The finding challenges conventional wisdom that privacy worries automatically translate into usage avoidance.

Trust (H8) maintains its significant positive influence, functioning as a crucial mediator between risk recognition and continued engagement. Users can simultaneously acknowledge potential threats while maintaining strong usage intentions when trust levels remain high. The relationship suggests that trust operates as a psychological buffer, allowing individuals to navigate uncertainty while pursuing desired benefits. Previous research in Indonesian digital payment adoption consistently identifies trust as a fundamental factor, and these results reinforce its enduring importance across different theoretical frameworks. The rejection of Security (H6) and Self-Efficacy (H7) hypotheses offers equally valuable insights into user psychology. Perceived security features fail to achieve statistical significance, suggesting that users may struggle to understand or properly evaluate technical protection measures. Rather than being impressed by sophisticated security technologies, users appear more responsive to outcome-focused communications that build confidence in protective results. Self-efficacy also lacks significant impact, indicating that personal confidence in one's own protective abilities matters less than faith in service provider capabilities. Users seem willing to delegate security responsibilities to trusted platforms rather than relying on their own technical skills.

The R^2 value of 0.693 demonstrates that PMT explains approximately 69% of behavioral intention variance, leaving substantial room for additional influencing factors. Cultural dimensions, social proof mechanisms, or situational variables likely account for the remaining explanatory gap. Indonesian collectivist culture, where group opinions and social recommendations carry significant weight, may moderate individual risk-benefit calculations in ways not captured by traditional PMT constructs. Future research could explore how cultural values interact with protection motivation processes.

Practical implications for GoPay and similar digital payment providers emerge clearly from these findings. Privacy communications should emphasize protective capabilities and successful threat mitigation rather than attempting to minimize or dismiss legitimate concerns. Trust-building initiatives deserve priority over technical security feature promotion, as users respond more strongly to relationship-based confidence than technical specifications. Response cost considerations require careful attention to ensure users perceive security measures as reasonable investments rather than burdensome obstacles to convenience. The research advances PMT literature by demonstrating successful application in digital payment environments within emerging markets. The positive relationships between threat perceptions and behavioral intentions challenge traditional risk-avoidance models that assume threat awareness leads to behavioral withdrawal. Instead, the findings support PMT's foundational premise that threat recognition can motivate protective engagement when users believe effective protection mechanisms exist. The study reveals how sophisticated users can simultaneously maintain risk awareness and usage intentions, provided they trust the protective framework surrounding their activities.

5. Conclusion

Based on the analysis of eight hypotheses, where six were accepted, the main conclusions of this research can be summarized as follows. GoPay usage intention is fundamentally shaped by risk perceptions and trust in offered solutions. Psychological factors such as Privacy Concern, Perceived Severity of threats, and personal Perceived Vulnerability prove to significantly drive adoption intentions. These drivers are reinforced by users' confidence in GoPay's effectiveness in mitigating risks (Response Efficacy), their willingness to bear non-financial "costs" for security (Response Cost), and the level of Trust that serves as the primary foundation of the user-service relationship. Service security features and individual capabilities are not the main driving factors for behavioral intention. This research finds that perceptions of Security features and confidence in one's own abilities (Self-Efficacy) do not have significant influence. This implies that security aspects may already be considered minimum standards (hygiene factors) by users, no longer serving as differentiating values. Additionally, users tend to rely more on security systems provided by GoPay rather than their personal capabilities to protect themselves, making self-efficacy less of a primary consideration. The research confirms that GoPay usage behavioral intention is significantly shaped by risk evaluation and trust processes, as explained by Protection Motivation Theory. Psychological factors such as privacy concerns, threat perceptions (severity and vulnerability), GoPay's response effectiveness, and trust are the main drivers. Conversely, general perceptions of Security features and confidence in one's own abilities (Self-Efficacy) are not significant driving

factors. This implies that user decisions depend more on their trust in the service provider's protection system rather than personal technical capabilities or security features that are considered standard.

The findings reveal that users engage in sophisticated risk-benefit calculations where threat awareness paradoxically strengthens rather than weakens usage intentions. When individuals recognize potential dangers but simultaneously trust the protective mechanisms in place, they demonstrate higher engagement levels. This pattern suggests that effective digital payment adoption strategies should focus on building institutional trust and demonstrating protective capabilities rather than minimizing risk discussions or emphasizing technical security features that users may not fully understand or appreciate.

References

[1] Annisa, & Munas Dwiyanto, B. (2021). Analisis pengaruh kualitas layanan dan kepercayaan terhadap loyalitas pelanggan dengan kepuasan pelanggan sebagai variabel mediator (Studi pada pengguna jasa PT. Pos Indonesia di Semarang). *Diponegoro Journal of Management*, *10*(3), 1–12.

[2] Delima Sari, S. (2023). Privasi dan keamanan data dalam statistik resmi: Tantangan dan solusi dalam perlindungan data individu. *Jurnal Ilmiah Multidisipline*, *1*(11), 700–703. https://doi.org/10.5281/zenodo.10371661

[3] Fitriawibowo, W. A., & Kusumawati, E. (2024). Minat Penggunaan Sistem Pembayaran Shopeepay Sebagai Dompet Digital. *Innovative: Journal Of Social Science Research*, *4*(1), 4710-4719. https://doi.org/10.31004/innovative.v4i1.8411

[4] Garland, R. (1991). The mid-point on a rating scale: Is it desirable. *Marketing bulletin*, *2*(1), 66-70.

[5] Gatot Efrianto, & Nia Tresnawaty. (2021). Pengaruh privasi, keamanan, kepercayaan dan pengalaman terhadap penggunaan fintech di kalangan masyarakat Kabupaten Tangerang Banten. *Jurnal Liabilitas*, *6*(1), 53–72. https://doi.org/10.54964/liabilitas.v6i1.71

[6] Ghozali, H. L. (2020). *Partial least squares: Konsep, teknik dan aplikasi menggunakan SmartPLS 3.0 untuk penelitian empiris*. Badan Penerbit Universitas Diponegoro.

[7] Ghozali, I. (2016). *Aplikasi analisis multivariete dengan program IBM SPSS 23* (8th ed.). Badan Penerbit Universitas Diponegoro.

[8] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2013). *Multivariate data analysis: Pearson new international edition PDF eBook*. Pearson Higher Ed.

[9] Jamiah, N., Purwanto, H., & Asmike, M. (2022). Pengaruh persepsi kemudahan penggunaan dan keamanan terhadap minat menggunakan melalui kepercayaan sebagai variabel intervening (Studi empiris pada e-wallet GoPay di Kota Madiun). *Seminar Inovasi Manajemen Bisnis dan Akuntansi 4*, 1–19.

[10] Kamil, L. I. (2019). *Pengaruh kepercayaan, keamanan dan persepsi kemudahan penggunaan terhadap minat untuk menggunakan GoPay* [Undergraduate thesis]. Institut Agama Islam Negeri Surakarta.

[11] Kumala, M. (2020). Peran dompet digital dalam meningkatkan kualitas keuangan UMKM menuju era Society 5.0. *JPM: Jurnal Pengabdian Masyarakat*, *4*(1), 26–34. https://doi.org/10.47065/jpm.v4i1.859

[12] Liani, A. M., & Yusuf, A. (2021). Pengaruh e-trust terhadap e-loyalty dimediasi oleh e-satisfaction pada pengguna dompet digital GoPay. *YUME: Journal of Management*, *4*(1), 138–149. https://doi.org/10.37531/yume.vxix.445

[13] Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. *TheoryHub Book: This handbook is based on the online theory resource: TheoryHub*, 78-93.

[14] Nowlis, S. M., Kahn, B. E., & Dhar, R. (2002). Coping with ambivalence: The effect of removing a neutral option on consumer attitude and preference judgments. *Journal of Consumer Research*, *29*(3), 319–334. https://doi.org/10.1086/344431

[15] Prasetyo, A., & Wardhani, A. M. N. (2022). Analisis pengaruh perceived risk dan trust terhadap pengujian behavioral intention mahasiswa pengguna GoPay. *EXERO: Journal of Research in Business and Economics*, *5*(1), 36–63. https://doi.org/10.24071/exero.v5i1.5038

[16] Sugiyono. (2011). *Metodologi penelitian kuantitatif kualitatif dan R&D*.

[17] Sukmawati, K., & Kowanda, D. (2022). Keputusan penggunaan e-wallet GoPay berdasarkan pengaruh keamanan, persepsi kemudahan dan persepsi manfaat. *Jurnal Ilmiah Multidisiplin*, *1*(05), 66–72. https://doi.org/10.56127/jukim.v1i05.481

[18] Yam, J. H., & Taufik, R. (2021). Hipotesis penelitian kuantitatif. *Perspektif: Jurnal Ilmu Administrasi*, *3*(2), 96–102.

[19] Zaman, M. B., Pamungkas, I. B., & Wibowo, W. A. (2022). Pengaruh privasi dan keamanan terhadap penggunaan mobile payment. *SCIENTIFIC JOURNAL OF REFLECTION: Economic, Accounting, Management and Business*, *5*(4), 891–902. https://doi.org/10.37481/sjr.v5i4.565.