

# An Empirical Investigation of Factors Affecting Personal Information's Disclosure on Mobile Payment (E-Wallet) Platforms

Ashma Hanifah Shalihah<sup>a</sup>, Yova Ruldeviyani<sup>a,\*</sup>, Karisa Saraswati<sup>a</sup>, Abhimata Ar Rasyiid<sup>a</sup>

<sup>a</sup> Faculty of Computer Science, Universitas Indonesia, Jakarta, 10440, Indonesia

Corresponding author: \*yova@cs.ui.ac.id

**Abstract**— Along with the growing number of smartphone users, applications on mobile devices have progressed rapidly. The financial sector is one of the sectors affected by these technological advances. Digital payment is part of a financial application that is commonly used by the public. Coupled with the Covid-19 pandemic, transaction payment methods using mobile payment (e-wallet) platforms have also increased. In practice, e-wallets require users' personal information. This research aims to investigate factors that affect the intention of users to share their personal information on e-wallet platforms. This study tested six factors: personalized service, convenience, privacy settings control, familiarity, perceived benefit, and perceived privacy. These factors formed the basis of a research model and the proposed set of hypotheses. The data was collected through an online survey, and several 255 respondents provided valid responses. Using structural equation modeling, the SmartPLS application was used as a tool to process and analyze the survey data. The results of this study indicate that all hypotheses are accepted. This means perceived benefits and privacy from the user's side positively influence users' intentions to disclose their personal information regarding the use of e-wallet applications. Moreover, perceived benefit is impacted by personalized service and convenience factors. Meanwhile, perceived privacy is impacted by privacy settings control and familiarity factors. The findings and analyses are expected to allow fintech researchers to use prior work with adequate clarity, leading to improved rigid hypotheses in the future.

**Keywords**— Mobile payment; e-wallet; disclosure of personal information; PLS-SEM.

Manuscript received 12 Jul. 2022; revised 7 Nov. 2022; accepted 20 Nov. 2022. Date of publication 30 Jun. 2023.  
IJASEIT is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.



## I. INTRODUCTION

A mobile application is software installed and runs on a mobile device or smartphone. Advances in these applications obtained a rapidly increasing number of users with mobile devices or smartphones [1]. These advances also had a direct impact on the financial sector, such as the provision of services through mobile applications and a combination of "Finance" and "Technology" known as Fintech [2]. Furthermore, the rapid development of this fintech in Indonesia led to the digital payment of its growing sectors [3], [4]. Digital or mobile payments through a mobile application are viable to the convenience offered [5]. The widespread use of fintech has shifted how financial transactions are carried out. The Covid-19 pandemic increased the number of payment transactions carried out using mobile applications, reducing the spread of the virus compared to cash payments. People saving money with an e-wallet in mobile payment applications also increased [6].

Moreover, the Indonesian government launched the National Non-Cash Movement (GNNT) program through Indonesian banks in 2014 to obtain a Less Cash Society for the people [7]. Ae-wallet requires user's personal information such as profile data, credit card information, shopping preferences, phone numbers, and history [8]. Therefore, users indirectly publish personal information on application providers, which may lead to the mismanagement of data or data leakage by the providers [9]. In 2019, about 22% of digital payment platforms in Indonesia dealt with system failures and cyberattacks [10].

Several previous studies have discovered a strong relationship between privacy concerns and the disclosure of personal information [11], [12]. Additionally, privacy concern often arises when it comes to the collection and use of personally identifiable information [13]. According to another study, some individuals perceive the collection, use, and sharing of personal information as a major threat to Internet users, and it influences protective behaviors toward privacy [14]. Meanwhile, in the case of e-commerce, online

privacy concerns can trigger defensive behavior in customers, such as hiding personal information and falsifying personal information [15].

Furthermore, different research explained that experienced users' intentions to use mobile wallet services are positively influenced by perceived security and relative advantages [16]. While security awareness has become an essential element for treating online users' concerns [17], it has been discovered that users will continue to use mobile payments based on cognitive perceptions of perceived security and trust in mobile payments [18]. Another study supported that data security is the greatest impediment to adopting fintech innovations because it has a substantial influence on trust [2], [19], [20], and due to the large number of emerging technologies related to Fintech platforms, it is difficult to perceive all of the potential cyber risks [21].

Based on the issue of the rapid growth of fintech and numerous factors that may impact information disclosure, various e-wallet service providers should prioritize the security of user data, in addition to understanding user behavior and their willingness to disclose personal information online. As a result, this study was conducted to investigate factors that affect the intention to disclose personal information on online fintech platforms, especially e-wallets. Besides that, this study examined two factors, namely perceived privacy, and benefit. It also specifically addressed two questions (RQ) as follows:

- RQ1. What privacy dimensions affect the disclosure of user's personal information?
- RQ2. What benefits are expected to encourage the disclosure of user's personal information?

To answer these two questions, a research model on user's intentions to disclose personal information during the use of e-wallet applications was developed based on theories from existing studies. This study was the first of its kind in Indonesia. The remainder of this paper is coordinated into four chapters. Following the Introduction, the second chapter explains about the materials and method used to employ this study, the third chapter presents the results and discussion, and the last chapter provides the conclusion of this research.

## II. MATERIALS AND METHOD

### A. Research Model and Hypotheses Development

The research model for disclosing personal information was developed with the following six hypotheses. A personalized service is a form of service customized for users based on personal information. Regarding mobile banking services, personalized services facilitate financial transactions more quickly and easily. They can also help users interact with the services more effectively and efficiently, increasing their satisfaction level [22]. Here, users are accustomed to exchanging personal information to obtain special services from service providers.

These services may include special discounts or product recommendations. Users benefit from having recommendations that are reasonable and appropriate for their needs, which makes it easier for them to select the proper products. They spend less time searching as a result, and they value these advantages [23]. From the special services obtained, users understand the benefits of sharing personal

information on their applications [24]. Moreover, personalization is seen as a general benefit and situational incentive for influencing customers' perceptions of data disclosure [25]. This forms the basis of the hypothesis below:

1) *H1*: Personalized service positively influences the user's perceived benefits, provided personal information is disclosed. According to one study, convenience encourages users to disclose their information [26], [27]. It was said that mobile payments are both safer and more convenient than cash transactions. People can pay their bills whenever and wherever they choose thanks to online payment over the internet [28]. Additionally, despite being aware of the important privacy concerns, people continue to provide their personal data in order to access some convenient utilities [29]. Those lead to the formation of the following hypothesis:

2) *H2*: Convenience positively influences the user's perceived benefits, provided that personal information is disclosed. The effectiveness of user privacy settings or control has a positive psychological effect on information disclosure. One of these controls is the power to decide how to use and restrict some personal information. Users have control over the data submitted into the system and retrieved from it [30]. In another study, privacy control refers to the user's ability to independently select which personal information can be collected and used by the e-wallet application [31]. Through the platform's privacy practices, a user can learn how it manages personal information and ensures data security. Additionally, privacy control is often regarded as a vital variable in relation to attitude when people are making trade-off decisions, and as a result, it has been incorporated into models related to privacy [32]. The impact of privacy controls was that users were less worried about data access and unauthorized data use. Users may also have a low level of control over personal information while using mobile payment applications that do not have privacy settings. Moreover, a prior study also found that better transparency regarding the sorts of data requested, and the purpose of their use could eventually affect the individual's concern and disclosure attitude [33]. Thus, another study hypothesis is formed as follows:

3) *H3*: Privacy setting controls positively influence the perceived privacy of users, provided that personal information is disclosed. Familiarity with the application will determine the level at which the e-wallet application is widely adopted and recognized. A study by Wirani [34] explained that customers' propensity to use Fintech services in Indonesia is influenced by the reliability of service providers with a precise and reputable reputation. It was also found that familiarity has a negative effect related to user privacy concerns [9]. In this e-wallet case study, an individual develops familiarity with an application that has been used or seen previously. However, the reverse occurs for an application that has not been used. This foundation forms the basis of the following hypothesis:

4) *H4*: Familiarity with the application positively influences the user's perceived privacy, provided that personal information is disclosed. Perceived benefit refers to the user's awareness of the benefits that can be obtained upon disclosing personal information [35], [36]. One of the main functions of

e-wallet applications is to provide payment services [37]. When using the application, users are prompted to provide relevant data, including location data, personal profiles, and purchasing preferences. While the perceived benefits of granting access to personal data tend to outweigh privacy worries and the costs associated with privacy protection [38], it allows users to obtain personal and useful financial services. These facilities or perceived benefits are an added value for users that disclose personal information on the application [31]. Therefore, this study designed the following hypothesis:

5) *H5*: Perceived benefits positively influence users' intention to disclose personal information. Users concerned about their privacy, particularly when using online platforms, are less likely to share their personal information [11]. The negation of this forms the basis of the hypothesis below:

6) *H6*: Perceived privacy positively influences the user's intention to disclose personal information. The six hypotheses listed above served as the foundation for the research model depicted in Figure 1.

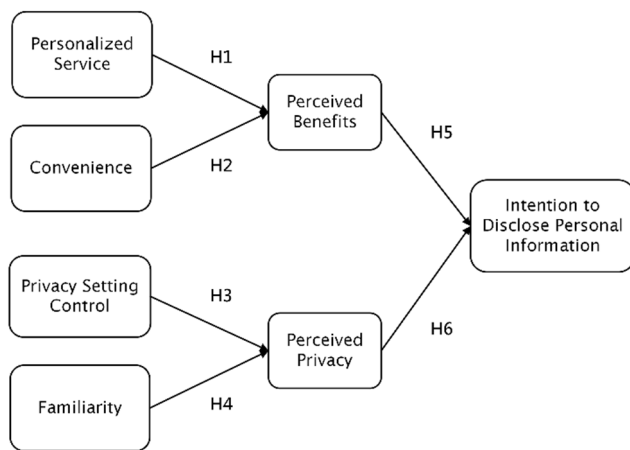


Fig. 1 User's information disclosure intention model

### B. Data Collection and Analysis

A web-based questionnaire was used to investigate the factors that influenced the disclosure of personal information on a mobile payment platform (e-wallet). The questionnaire consisted of four main sections. The first part obtained general information from respondents, such as age, gender, work type, and experience while using e-wallet applications. The second part required respondents' opinions about the applications' perceived benefits. The second part to the end of the questionnaire contained the measurement of the hypotheses.

The third part includes questions regarding respondents' perceptions of data privacy using e-wallet applications. The fourth part was intended to assess the disclosure of user information to the applications. Each question contained various items measured on a five-point Likert scale from (1) "Strongly disagree" to (5) "Strongly agree".

This online survey was used as a data collection instrument for this investigation. It was distributed to target users of e-wallet applications such as Gopay, OVO, Dana, ShopeePay, and LinkAja in Indonesia. These five applications were

selected as reference platforms to test the proposed model due to their popularity among Indonesians. This data was obtained from market share surveys showing a dominating prominence when compared to other applications in Figure 2.

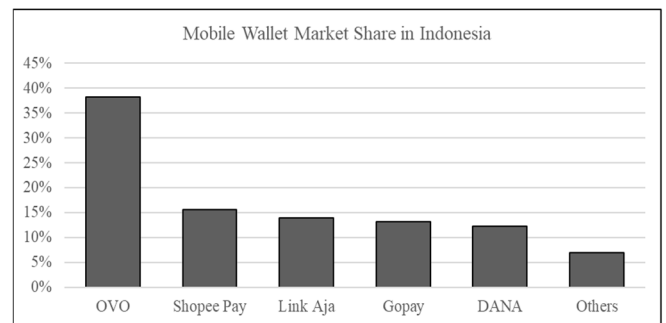


Fig. 2 E-wallet Market Share in Indonesia [39]

The questionnaire is built on the research model that was developed. Moreover, the data results obtained from the questionnaire distribution were used as input for testing the study framework. To maximize the number of responses, this study also used messenger applications to spread the questionnaire link.

The sample for this study has been approved as comprising 255 respondent data in total. Personalized service, convenience, control over privacy setting, familiarity, perceived benefits, perceived privacy, and intention to disclose personal information are among the variables that the research model (Figure 1) combined to identify factors affecting users' intention to disclose their personal information while using an e-wallet application.

Earlier validated scales were used to measure these factors. The personalized service measurement was derived from Xu et al. [40], while Al-Jabri et al. [26] adopted the convenience variable. The intention to share personal information was adapted from Wang et al. [24], while the privacy setting control variable was adapted from Yang et al. [31], familiarity from Wang et al. [41], perceived benefits from Lin et al. [42], and the perceived privacy was from Najjar et al. [43].

Most of those measurement items were adopted and modified from previous relevant literature (see Table I), which are then used as input for the data analysis process. The PLS-SEM approach was used in this study to examine and validate the suggested research model.

### III. RESULTS AND DISCUSSION

The questionnaire was distributed by sharing links online, and from the responses we received, Table II shows the demographic information about the respondents. During the data processing process, this research used the statistical software SmartPLS3. The approach steps that are applied when processing the data are divided into two; the first step involves evaluating the measurement model by assessing convergent validity, discriminant validity, and measuring reliability. The second step is to evaluate the structural equation model, examine the hypotheses made, and determine the relationship between each factor involved.

TABLE I  
FACTORS USED IN THE RESEARCH MODEL

Measured Items	Source
<b>Personalized Service</b>	
The e-wallet application provides personalized offers tailored to the context of individual activity.	[40]
The e-wallet application provides promotional information relevant to my personal preferences.	
The e-wallet application provides potential offers which I might like.	
<b>Convenience</b>	
Making transactions on the e-wallet app allows me to save my time.	[26]
Using the e-wallet application is a convenient way of saving my money to make transactions.	
I can use the e-wallet application to save money and carry out transactions anywhere.	
<b>Privacy setting control</b>	
The personal information that will be collected by e-wallet application can be easily controlled.	[31]
The personal information used by the e-wallet application can be effectively controlled.	
The personal information provided to the e-wallet application can be independently chosen.	
<b>Familiarity</b>	
The e-wallet application used is quite popular.	[41]
The e-wallet application used is widely recognized.	
The e-wallet application used has a good reputation.	
<b>Perceived Benefits</b>	
Considering the effort expended, using an e-wallet, it is personally beneficial.	[42]
The use of an e-wallet is personally valuable.	
<b>Perceived Privacy</b>	
Personally certain about how my privacy is protected on the e-wallet application used.	[43]
The personal information cannot be misused while using the app.	
Personally unbothered by the requirement of the e-wallet app to provide personal information.	
<b>Intention to Disclose Personal Information</b>	
I am likely to disclose personal information on e-wallet applications.	[24]
Willingness to disclose personal information on the e-wallet application is present.	
Personal information disclosure for e-wallet product and service is possible for me.	

TABLE II  
RESPONDENT PROFILE

Profile	Item	Frequency	Percentage
Gender	Male	145	56.9%
	Female	110	43.1%
Age	20-24 years old	11	4.3%
	25-29 years old	51	20%
	30-34 years old	61	23.9%
	35-39 years old	18	7.1%
	≥ 40 years old	114	44.7%
Educational background	Senior High School	5	2%
	Bachelor's Degree (S1)	171	67.1%
	Master's degree (S2)	79	31%
Work	Student	5	2%
	Government employees	78	30.5%
	Private employees	121	47.5%
	Entrepreneur	25	9.8%
	Housewife	11	4.3%
Monthly Income (in IDR)	Other	15	5.8%
	< 5,000,000	25	9.8%
	5,000,000-9,999,999	87	34.1%
	10,000,000-14,999,999	43	16.9%
	15,000,000-19,999,999	33	12.9%
	20,000,000-24,999,999	10	3.9%
Application usage time	≥ 25,000,000	57	22.4%
	0-1 years	17	6.7%
	2-3 years	118	46.3%
	4-5 years	76	29.8%
	> 5 years	44	17.3%
Frequency of app use	Every day	76	29.8%
	Every week (3-5 times per week)	111	43.5%
	Every month (3-5 times per month)	68	26.7%

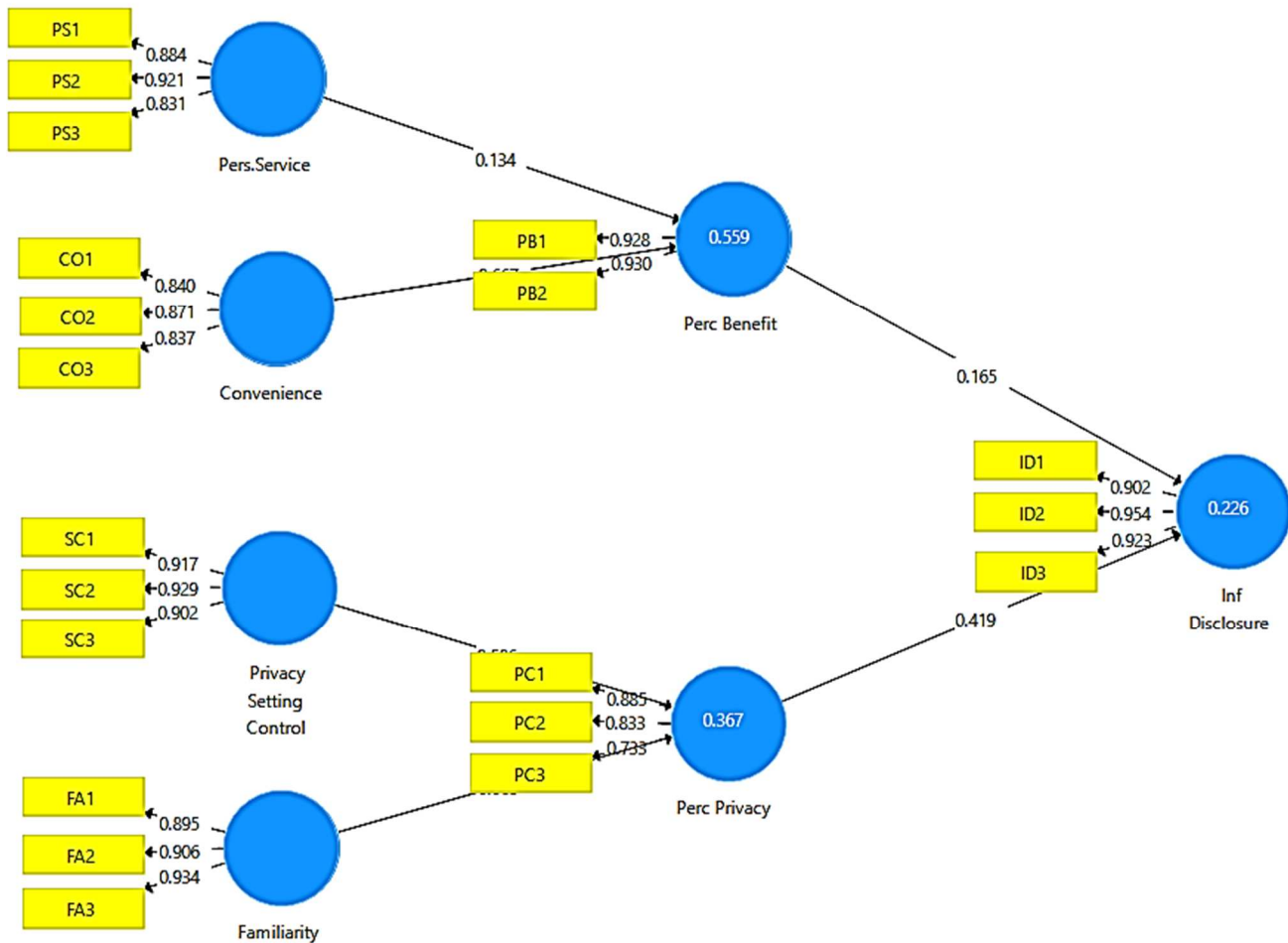


Fig. 3 Result of PLS algorithm

This study compiled a structural equation model (SEM), which was built on seven latent variables (PS / Personalized Service, CO / Convenience, SC / Privacy Setting Control, FA / Familiarity, PB / Perceived Benefits, PC / Perceived Privacy, ID / Intention to Disclose Personal Information). Figure 3 depicts the execution of the PLS algorithm.

Testing the validity and reliability of the research instruments is done to evaluate the measurement model. If the convergent validity test and discriminant validity test requirements are satisfied, the model is said to be valid. The outcome of the convergent validity test is viewed as the loading factor value in factor analysis.

The expected result while evaluating the convergent validity is more than 0.7. As a material for interpreting the model structure, this value is the minimum limit of the factor load value [44]. If the result of the factor load is greater, then the indicator is regarded as significant or has a significant value for the factor studied [45]. Table III demonstrates that the total factor loadings obtained match the convergent validity test condition because they are  $> 0.7$ .

In addition, convergent validity can also be examined by looking at the average extract variance (AVE) of each construct or latent variable. The construct is said to be valid if it passes the  $AVE > 0.5$  condition [44]. Each latent variable's AVE value is shown in Table III. All latent variables or constructs in this investigation exceeded the value of 0.5, indicating that they have high convergent validity.

TABLE III  
MEASUREMENT MODEL EVALUATION

Construct	Indicators	Loadings	AVE
Personalized Service	PS1	0,884	0,773
	PS2	0,921	
	PS3	0,831	
Convenience	CO1	0,840	0,721
	CO2	0,871	
	CO3	0,837	
Privacy Setting Control	SC1	0,917	0,839
	SC2	0,929	
	SC3	0,902	
Familiarity	FA1	0,895	0,831
	FA2	0,906	
	FA3	0,934	
Perceived Benefits	PB1	0,928	0,863
	PB2	0,930	
Perceived Privacy	PC1	0,885	0,672
	PC2	0,833	
	PC3	0,733	
Intention to Disclose Personal Information	ID1	0,902	0,859
	ID2	0,954	
	ID3	0,923	

The discriminant validity test evaluates the degree to which a construct differs from other constructs in the model. The

value used for comparison is the root of AVE. The research model has strong discriminant validity if the construct's AVE root is higher than its correlation value with other constructs. Table IV displays the result of the discriminant validity test.

TABLE IV  
AVE ROOT AND CORRELATION VALUE BETWEEN VARIABLES

	CO	FA	ID	PB	PC	PS	SC
<b>CO</b>	<b>0.849</b>						
<b>FA</b>	0.438	<b>0.912</b>					
<b>ID</b>	0.303	0.210	<b>0.927</b>				
<b>PB</b>	0.739	0.434	0.235	<b>0.929</b>			
<b>PC</b>	0.239	0.215	0.447	0.168	<b>0.820</b>		
<b>PS</b>	0.539	0.276	0.342	0.494	0.322	<b>0.879</b>	
<b>SC</b>	0.287	0.255	0.300	0.181	0.602	0.436	<b>0.916</b>

According to Table IV, the model has an adequate discriminant because each construct's AVE root has a value bigger than the correlation between that construct and the other constructs. In evaluating the measurement model, the next step needed is to test the reliability of the construct. The composite reliability test and Cronbach Alfa ( $\alpha$ ) are the reliability tests employed. The parameters commonly used in research are all composite reliability, and Cronbach Alpha values from each construct must be  $> 0.7$  [44], [46]. Table V confirms that all the constructs used in the study can be accepted or have good reliability to be used as research.

TABLE V  
RELIABILITY AND STRUCTURAL MODEL ANALYSIS

Construct	Composite Reliability	Cronbach Alpha ( $\alpha$ )	R <sup>2</sup>
Personalized Service	0,911	0,853	-
Convenience	0,886	0,807	-
Privacy Setting Control	0,940	0,904	-
Familiarity	0,937	0,908	-
Perceived Benefits	0,926	0,841	0,559
Perceived Privacy Intention to Disclose Personal Information	0,859	0,752	0,367
	0,948	0,918	0,226

The structural model will next be assessed by looking at the R-square value [44]. In Table V, the R-square column for the perceived benefits variable shows that as much as 55.9% of the variance proportion of the construct can be explained by the variables of personalized service and convenience. In comparison, the R-square value for the perceived privacy variable shows that as much as 36.7% of the variance proportion of the variable can be explained by the familiarity variable and the privacy control settings.

The perceived benefits and perceived privacy variables account for 22.6 percent of the variance in the intention to disclose personal information variable, according to the R-square column for this variable. Among the three endogenous variables in this research model, the PB variable can be

explained more by the two exogenous variables when compared to the PC or ID variables.

The influence of the relationship between exogenous latent variables and endogenous latent variables can also be seen from the path coefficient generated in SmartPLS. Table VI shows the total path coefficient values for each latent variable, while Table VII shows the summary results of the hypothesis testing of the research model.

TABLE VI  
PATH COEFFICIENT FROM THE RESEARCH MODEL

Latent Variable Relationship	Path Coefficient	Standard Deviation (STDEV)	T Statistic ( O/STDEV )
PS $\rightarrow$ PB	0,134	0,035	3,814
CO $\rightarrow$ PB	0,667	0,035	19,029
SC $\rightarrow$ PC	0,586	0,036	16,172
FA $\rightarrow$ PC	0,067	0,032	2,067
PB $\rightarrow$ ID	0,165	0,052	3,187
PC $\rightarrow$ ID	0,419	0,042	9,993

Table VI shows that the latent variable PS has a positive relationship with the latent variable PB. This is demonstrated by the latent variable PS and PB's path coefficient value, which is 0.134 (path coefficient  $> 0$ ), and the T-statistic value, which is 3.814. In testing this model, it can be said that the PS variable affects the PB variable because the minimal T-value typically employed for a significance level of 5% is 1.96 [44], indicating that when testing this model, it is reasonable to infer that the PS variable positively influences the PB variable.

Meanwhile, with a path coefficient value of 0.667 and a T-statistic of 19,029, which is higher than the value of 1.96 for a significance level of 5%, the relationship between the latent variables CO and PB, may be stated to influence PB. A positive path coefficient value means the relationship between the CO and PB is linear.

The PC latent variable is positively impacted by the SC variable as well. SC demonstrates this to the PC path coefficient value, 0.586, and the T-statistic, 16,172. The path coefficient is positive, showing that the SC value is directly proportional to PC, and the t-statistic  $> 1.96$  shows that the SC latent variable influences PC.

The relationship between the latent variable FA and the latent variable PC has a path coefficient value of 0.067 with a t-statistic of 2.067, greater than the value of 1.96 for a significance level of 5%. Since the value of the FA variable is directly proportional to the value of the PC variable, it can be stated that FA impacts PC.

For the relationship between the latent variable PB and ID, the path coefficient of 0.165 shows that the value of the latent variable PB is directly proportional to the latent variable ID. The latent variable PB also influences the ID variable, according to the t-statistic value of 3.187. Additionally, the latent variable PC influences the latent variable ID positively. This could be observed from SC to PC route coefficient, which has a t-statistic value of 9.993 and a value of 0.419.

Because the t-statistic is more than 1.96, it can be implied that the latent variable PC affects ID, and as long as the path coefficient is positive, it can be assumed that the PC value is directly proportional to ID.

In order to test the prepared hypotheses, P-Value is used as a parameter in the research that develops a PLS-SEM structural model [44]. In this investigation, testing was done at a 5 percent significance level, where if the  $p\text{-value} > 0.05$ , then the proposed hypothesis was rejected. The results of hypotheses testing are described in Table VII and summarized in Figure 4.

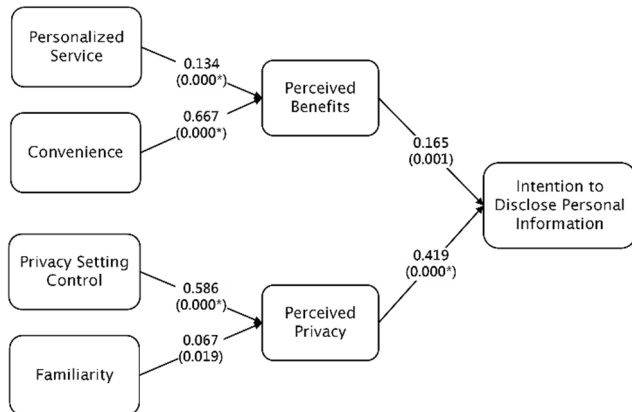


Fig. 4 Result of hypotheses testing

The results of hypothesis H1 show a  $p\text{-value} < 0.001$ . Because the  $p\text{-value} < 0.05$ , the test results support the proposed hypothesis. This shows that personalized service is a significant variable in the benefits perceived by users. This hypothesis confirms other research, which stated that there is a tendency for users to share personal information when they get customization or special types of personal services from applications that users use or take advantage of [24].

In H2, the  $p\text{-value}$  displays a result less than 0.001, supporting the hypothesis for H2. This demonstrates that the benefits or advantages experienced by the user when using the e-wallet application are significantly influenced by their level of convenience utilizing the application. These findings are consistent with earlier research that support how consumer convenience affects their desire to provide personal information [26]–[29].

Hypothesis H3 shows a  $p\text{-value} < 0.001$ , which confirms the hypothesis. This indicates that the control of privacy settings in using the e-wallet application significantly impacts the privacy users feel when using the application. According to the research that forms the basis for the research hypothesis in this study, users believe that their personal information cannot be misused since they have control over the personal information that the application would acquire [47].

The result of hypothesis H4 shows the value of  $p = 0.019$ . This finding of the H4 test can be interpreted as supporting the stated hypothesis because this  $p\text{-value}$  is below the threshold of 0.05. From the finding, it can be concluded that the familiarity variable significantly influences consumers' perceptions of privacy when using an e-wallet application. This evidence supports a recent study stating that familiarity variables significantly influence how users think about their privacy [9].

TABLE VII  
HYPOTHESES RESULTS

Hypotheses	P-value	Results
H1: Personalized Service → Perceived benefits	0.000*	Significant, accepted
H2: Convenience → Perceived benefits	0.000*	Significant, accepted
H3: Privacy Control Settings → Perceived privacy	0.000*	Significant, accepted
H4: Familiarity → Perceived privacy	0.019	Significant, accepted
H5: Perceived benefits → Intention to Disclose Personal Information	0.001	Significant, accepted
H6: Perceived privacy → Intention to Disclose Personal Information	0.000*	Significant, accepted

Note, \* $p$  value  $< 0.001$ .

According to the findings of hypothesis H5,  $p = 0.001$  was obtained. The  $p\text{-value}$  is still worth  $< 0.05$ , so hypothesis H5 is declared accepted. This indicates that the perceived benefit variable significantly affects the intention to share information by users of the e-wallet application. Therefore, if someone experiences the advantages of utilizing an e-wallet feature, it increases their motivation to share personal information since they believe there is more value to be gained from using the application. This finding is consistent with a study that forms the foundation for this hypothesis [31]. It is also similar to another previous research, which stated that perceived benefit is an essential factor influencing attitudes toward information technology [45].

Hypothesis H6 is supported by the findings, which have a  $p\text{-value}$  of less than 0.001. It reflects that the perceived privacy variable significantly influences users of the e-wallet application's intention to share personal information. This suggests that when someone is aware of the privacy practices available in the application, it increases their desire to disclose their information on the e-wallet application since they feel secure. This hypothesis is consistent with previous results by Gong et al. [8].

Based on the findings of this hypotheses test, it can be said that user's convenience, personalized service, familiarity, and control over privacy settings on the application can provide privacy and the benefits they feel and can increase their intentions to provide their personal information to the e-wallet applications. In the design of this study, one of the privacy variables that affect the user's intention to provide personal information is the privacy setting control. This indicates that if users are careful about their data privacy settings, they can prefer access restrictions and what types of information they share on e-wallet applications. Meanwhile, one benefit that affects the user's intention to provide personal information is the convenience dimension. A complete definition of convenience refers to the availability of applications to save time and practical access wherever and whenever the user requires the e-wallet application functions.

In designing this research, it was also found that two other variables influence the consumer's intention to disclose personal information, namely the familiarity variable and the personalized service variable. A possible explanation for the significance of the familiarity dimension to perceived privacy is that in Indonesia, the public's e-wallet applications are limited to a few applications. Applications that are common or the majority used by the public include OVO, Dana, GoPay, ShopeePay, and LinkAja.

In the survey data collected, more than 62% of respondents became multiuser on the e-wallet above applications. In other words, they use more than one e-wallet app to fulfill their financial needs. Respondents rated these applications as having a high level of popularity, and respondents rated themselves as familiar with the applications they used.

On the other hand, there is a need for personal data that is similar from one application to another, causing users to feel a significant similarity in data privacy from the applications used. So that users are not worried about privacy issues when using the application and can focus on using the application's main features, such as the e-wallet feature as a means of payment at various merchants.

For the personalized service variable, a possible explanation for its significance to the perceived benefit variable is that users of the e-wallet application prioritize the functionality of the e-wallet application so that the provision of personal information gradually becomes a necessity that needs to be done to obtain other features or services that are still related to the main function of the application (i.e., as a means of payment or bank transfers). This can also occur due to significant visible differences, from application providers in sharing their services to users who have or have not shared their personal data.

This study has several limitations; firstly, most of the survey responses came from respondents over 40 years and over. Most responders are also workers, including government and private sector workers. In addition, the highest frequency of respondents' monthly wage indicators is 5-10 million rupiahs, and the next highest position is at > 25 million rupiahs per month. It may also reflect disparities in the socioeconomic status of less diversified respondents because there are differences in the frequency of monthly wage ranges, which are less evenly distributed within range categories. These factors may impact the answers to the questions posed because user behavior and habits vary depending on their profile or background.

#### IV. CONCLUSION

This study aims to investigate the factors affecting a person's intention to disclose his personal information on an e-wallet platform. In this study, six variables were considered as factors. The six factors are personalized service, convenience, perceived benefits, privacy settings control, familiarity, and perceived privacy. Following compiling these variables into hypotheses, a research model is created.

Survey-based data collection was aimed at e-wallet application users in Indonesia to test the research model. From the data analysis carried out, there are interesting findings: in terms of sharing personal data, there are factors that have a positive impact on the intention to disclose information related to the use of e-wallet applications, namely

personalized service factor, convenience factor, familiarity factor, privacy setting control factor, perceived benefits factor, and perceived privacy from the user side. All factors in this research model significantly influence the intention of personal information disclosed by users.

This research has implications that can also be used as input for e-wallet service providers. The results of data analysis confirm that users tend to share their personal information if the e-wallet application they use is perceived to have more value for them, namely in terms of convenience and personal service. In addition, the privacy assurance approach is an effective strategy for overcoming privacy problems and the problem of disclosing personal information from consumers using e-wallet applications. Consumers are less likely to experience privacy concerns and are more likely to disclose their personal information to apps when they are offered an approach to privacy features that can guarantee or make them feel confident that the apps can protect the privacy of their information.

E-wallet service providers can strengthen the attributes of their applications, which positively impact or increase users' disposition to share their personal information. The perceived benefits can be supported by emphasizing the ease of use of the money storage feature and payment transactions that provide convenience when consumers use the e-wallet application. Meanwhile, in terms of privacy, service providers can establish clear procedures or standards regarding sharing users' personal data. This can serve as an overview for users regarding the limits on how much information they provide will be stored by the e-wallet service provider (application).

The results of this research analysis also recommend service providers improve the features of the decision-making mechanism for users in using the application to determine whether users are willing to share or provide access to their personal information while using the application. To create a safe environment for using the service, maintain user trust, and confirm the existence of applicable laws relating to personal information stored electronically, e-wallet service providers can also develop data privacy policies, which can then be disseminated to the wider community. For further research, this research provides several suggestions for development. Firstly, in terms of data sampling, subsequent research can expand the sample by utilizing a more diverse sample of age, type of work, and income to see the accuracy and generalizability of the model with larger demography. In addition, future research can also investigate e-wallet consumers' habits in sharing personal information by considering the types or variations of information they share when using e-wallet applications.

#### REFERENCES

- [1] L. Stocchi, N. Pourazad, N. Michaelidou, A. Tanusondjaja, and P. Harrigan, "Marketing research on Mobile apps: past, present and future," *J Acad Mark Sci*, vol. 50, no. 2, pp. 195–225, Mar. 2022, doi: 10.1007/S11747-021-00815-W/TABLES/5.
- [2] L. L. Zhang and H. K. Kim, "The influence of financial service characteristics on use intention through customer satisfaction with mobile fintech," *Journal of System and Management Sciences*, vol. 10, no. 2, pp. 82–94, 2020, doi: 10.33168/jsms.2020.0206.
- [3] K. Subaramaniam, R. Kolandaisamy, A. bin Jalil, and I. Kolandaisamy, "The impact of E-Wallets for current generation," *Journal of Advanced Research in Dynamical and Control Systems*,



- vol. 12, no. 1 Special Issue, pp. 751–759, 2020, doi: 10.5373/JARDCS/V12SP1/20201126.
- [4] A. A. Setiawan, Y. E. Silaen, T. Andreas, and T. Oktavia, “Analysis of Intention to Use on Pay Later Payment System During COVID-19 Pandemic,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 3, pp. 119–129, Mar. 2022, doi: 10.46338/IJETAE0322\_14.
- [5] G. Wang, N. M. Putri, A. Christianto, and W. Danny Hutama, “An empirical examination of characteristics of mobile payment users in Indonesia,” *J Theor Appl Inf Technol*, vol. 97, no. 1, pp. 169–182, Jan. 2019.
- [6] M. T. H. Le, “Examining factors that boost intention and loyalty to use Fintech post-COVID-19 lockdown as a new normal behavior,” *Heliyon*, vol. 7, no. 8, Aug. 2021, doi: 10.1016/J.HELIYON.2021.E07821.
- [7] B. Purwandari, S. A. Suriadin, A. N. Hidayanto, S. Setiawan, K. Phusavat, and M. Maulida, “Factors Affecting Switching Intention from Cash on Delivery to E-Payment Services in C2C E-Commerce Transactions: COVID-19, Transaction, and Technology Perspectives,” *Emerging Science Journal*, vol. 6, no. Special Issue, pp. 136–150, 2022, doi: 10.28991/ESJ-2022-SPER-010.
- [8] X. Gong, K. Z. K. Zhang, C. Chen, C. M. K. Cheung, and M. K. O. Lee, “What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity,” *Information Technology and People*, vol. 33, no. 4, pp. 1174–1213, Jun. 2020, doi: 10.1108/ITP-03-2018-0132.
- [9] G. Aiello *et al.*, “Customers’ Willingness to Disclose Personal Information throughout the Customer Purchase Journey in Retailing: The Role of Perceived Warmth,” *Journal of Retailing*, vol. 96, no. 4, pp. 490–506, Dec. 2020, doi: 10.1016/J.JRETAI.2020.07.001.
- [10] Asosiasi FinTech Indonesia (AFTECH), “AFTECH Annual Member Survey Report 2019/2020,” 2020. Accessed: Jan. 16, 2022. [Online]. Available: <https://fintech.id/dokumen/aftech-annual-member-survey-report-20192020>
- [11] V. Paramarta, M. Jihad, A. Dharma, I. C. Hapsari, P. I. Sandhyaduhita, and A. N. Hidayanto, “Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, twitter, and instagram,” *2018 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2018*, pp. 271–276, Jan. 2019, doi: 10.1109/ICACSIS.2018.8618220.
- [12] R. G. Anarak, K. A. Byrne, P. J. Wisniewski, X. Page, and B. P. Knijnenburg, “To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults,” *Conference on Human Factors in Computing Systems - Proceedings*, May 2021, doi: 10.1145/3411764.3445204.
- [13] K. B. Sheehan, “Toward a Typology of Internet Users and Online Privacy Concerns,” <https://doi.org/10.1080/01972240252818207>, vol. 18, no. 1, pp. 21–32, Jan. 2011, doi: 10.1080/01972240252818207.
- [14] S. C. Boerman, S. Kruikeijer, and F. J. Zuiderveen Borgesius, “Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data,” *Communication Research*, vol. 48, no. 7, pp. 953–977, Oct. 2021, doi: 10.1177/0093650218800915.
- [15] R. A. Mulia, F. Azzahro, and P. W. Handayani, “Analysis of internal and external factors affecting online privacy concern in E-commerce: Comparative study by gender,” *2020 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2020*, pp. 187–192, Oct. 2020, doi: 10.1109/ICACSIS51025.2020.9263227.
- [16] C. Mombeuil, “An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets,” *Journal of Retailing and Consumer Services*, vol. 55, Jul. 2020, doi: 10.1016/J.JRETCONSER.2020.102127.
- [17] M. S. Alif and A. R. Pratama, “Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia,” *AUTOMATA*, vol. 2, no. 1, Jan. 2021, Accessed: Jan. 16, 2022. [Online]. Available: <https://journal.uui.ac.id/AUTOMATA/article/view/17279>
- [18] L. A. Maureen Nelloh, A. S. Santoso, and M. W. Slamet, “Will users keep using mobile payment? It depends on trust and cognitive perspectives,” *Procedia Computer Science*, vol. 161, pp. 1156–1164, 2019, doi: 10.1016/J.PROCS.2019.11.228.
- [19] S. Mehrban *et al.*, “Towards secure FinTech: A survey, taxonomy, and open research challenges,” *IEEE Access*, vol. 8, pp. 23391–23406, 2020, doi: 10.1109/ACCESS.2020.2970430.
- [20] Z. Li, W. Li, Q. Y. Wen, J. Chen, W. Yin, and K. Liang, “An efficient blind filter: Location privacy protection and the access control in FinTech,” *Future Generation Computer Systems*, vol. 100, pp. 797–810, Nov. 2019, doi: 10.1016/J.FUTURE.2019.04.026.
- [21] E. Hernández, M. Öztürk, I. Sittón, and S. Rodríguez, “Data Protection on Fintech Platforms,” *Communications in Computer and Information Science*, vol. 1047, pp. 223–233, Jun. 2019, doi: 10.1007/978-3-030-24299-2\_19.
- [22] M. Albashrawi and L. Motiwalla, “Privacy and Personalization in Continued Usage Intention of Mobile Banking: An Integrative Perspective,” *Information Systems Frontiers*, vol. 21, no. 5, pp. 1031–1043, Oct. 2019, doi: 10.1007/S10796-017-9814-7/TABLES/7.
- [23] M. H. Nguyen and B. T. Khoa, “Customer electronic loyalty towards online business: The role of online trust, perceived mental benefits and hedonic value,” *Journal of Distribution Science*, vol. 17, no. 12, pp. 81–93, 2019, doi: 10.15722/JDS.17.12.201912.81.
- [24] T. Wang, T. D. Duong, and C. C. Chen, “Intention to disclose personal information via mobile applications: A privacy calculus perspective,” *International Journal of Information Management*, vol. 36, no. 4, pp. 531–542, Aug. 2016, doi: 10.1016/J.IJINFOMGT.2016.03.003.
- [25] M. H. J. Gouthier, C. Nennstiel, N. Kern, and L. Wendel, “The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce,” *Journal of Business Research*, vol. 148, pp. 174–189, Sep. 2022, doi: 10.1016/J.JBUSRES.2022.04.034.
- [26] I. M. Al-Jabri, M. I. Eid, and A. Abed, “The willingness to disclose personal information: Trade-off between privacy concerns and benefits,” *Information and Computer Security*, vol. 28, no. 2, pp. 161–181, Jun. 2020, doi: 10.1108/ICS-01-2018-0012/FULL/XML.
- [27] L. Yu, H. Li, W. He, F. K. Wang, and S. Jiao, “A meta-analysis to explore privacy cognition and information disclosure of internet users,” *International Journal of Information Management*, vol. 51, p. 102015, Apr. 2020, doi: 10.1016/J.IJINFOMGT.2019.09.011.
- [28] X. Cheng, T. Hou, and J. Mou, “Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing,” *Information & Management*, vol. 58, no. 6, p. 103450, Sep. 2021, doi: 10.1016/J.IM.2021.103450.
- [29] Y. Sun, F. Zhang, and Y. Feng, “Do individuals disclose or withhold information following the same logic: a configurational perspective of information disclosure in social media,” *Aslib Journal of Information Management*, vol. 74, no. 4, pp. 710–726, Jun. 2022, doi: 10.1108/AJIM-06-2021-0180/FULL/XML.
- [30] B. T. Khoa, “The Impact of the Personal Data Disclosure’s Tradeoff on the Trust and Attitude Loyalty in Mobile Banking Services,” *Journal of Promotion Management*, vol. 27, no. 4, pp. 585–608, 2020, doi: 10.1080/10496491.2020.1838028.
- [31] Q. Yang, X. Gong, K. Z. K. Zhang, H. Liu, and M. K. O. Lee, “Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms,” *International Journal of Information Management*, vol. 52, p. 102065, Jun. 2020, doi: 10.1016/J.IJINFOMGT.2019.102065.
- [32] Y. li Liu, W. Yan, and B. Hu, “Resistance to facial recognition payment in China: The influence of privacy-related factors,” *Telecommunications Policy*, vol. 45, no. 5, p. 102155, Jun. 2021, doi: 10.1016/J.TELPOL.2021.102155.
- [33] H. N. Chua, J. S. Ooi, and A. Herbrand, “The effects of different personal data categories on information privacy concern and disclosure,” *Computers & Security*, vol. 110, p. 102453, Nov. 2021, doi: 10.1016/J.COSE.2021.102453.
- [34] Y. Wirani, Randi, M. S. Romadhon, and Suhendi, “The influence of familiarity and personal innovativeness on the acceptance of fintech lending services: A perspective from Indonesian borrowers,” *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 1, pp. 81–93, Jan. 2022, doi: 10.26594/REGISTER.V8I1.2327.
- [35] K. Sutarno *et al.*, “Factors influencing user intention in opening personal data on social media,” *2020 5th International Conference on Informatics and Computing, ICIC 2020*, Nov. 2020, doi: 10.1109/ICIC50835.2020.9288614.
- [36] D. Pal, S. Funilkul, and X. Zhang, “Should I Disclose My Personal Data? Perspectives from Internet of Things Services,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3048163.
- [37] A. Sujana, D. P. Alamsyah, and S. M. Utomo, “The Continuous Usage of E-Wallet Support by Relative Advantage of Mobile Payment,” *2021 International Seminar on Machine Learning, Optimization, and Data Science, ISMODE 2021*, pp. 238–242, 2022, doi: 10.1109/ISMODE53584.2022.9743034.
- [38] M. Morimoto, “The Status Quo of Japanese Consumers’ Personal Information Disclosure: the Influence of Information Control and Privacy Concerns,” *Journal of International Consumer Marketing*, 2022, doi: 10.1080/08961530.2022.2059798.

- [39] "The 2021 Mobile Wallets Report from Boku," 2021. Accessed: Jan. 16, 2022. [Online]. Available: <https://boku.mobilewallet.report/>
- [40] H. Xu, H. H. Teo, B. C. Y. Tan, and R. Agarwal, "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *https://doi.org/10.2753/MIS0742-1222260305*, vol. 26, no. 3, pp. 135–174, Dec. 2014, doi: 10.2753/MIS0742-1222260305.
- [41] L. Wang, J. Yan, J. Lin, and W. Cui, "Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking," *International Journal of Information Management*, vol. 37, no. 1, pp. 1428–1440, Feb. 2017, doi: 10.1016/J.IJINFOMGT.2016.10.006.
- [42] K. Y. Lin, Y. T. Wang, and T. K. Huang, "Exploring the antecedents of mobile payment service usage: Perspectives based on cost–benefit theory, perceived value, and social influences," *Online Information Review*, vol. 44, no. 1, pp. 299–318, Jan. 2020, doi: 10.1108/OIR-05-2018-0175/FULL/XML.
- [43] M. S. Najjar, L. Dahabiyeh, and R. S. Algharabat, "Users' affect and satisfaction in a privacy calculus context," *Online Information Review*, vol. 45, no. 3, pp. 577–598, 2020, doi: 10.1108/OIR-02-2019-0054/FULL/XML.
- [44] Putu Wuri Handayani, Achmad Nizar Hidayanto, A. A. Pinem, and Fatimah Azzahro, *Konsep CB-SEM dan SEM-PLS: disertai dengan contoh kasus*. Depok: Rajawali Pers, 2019. Accessed: Jan. 16, 2022. [Online]. Available: <http://lontar.ui.ac.id>
- [45] M. Najib and F. Fahma, "Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium enterprises," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 10, no. 4, pp. 1702–1708, 2020, doi: 10.18517/IJASEIT.10.4.11616.
- [46] G. Prayitno, M. I. Ahari, and W. I. Rukmi, "Structural equation model with partial least square (SEM-PLS) of place dependence with land used change," *Journal of International Studies*, vol. 14, no. 1, pp. 153–171, 2021, doi: 10.14254/2071-8330.2021/14-1/11.
- [47] G. Mazurek and K. Małagocka, "What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think," *Business Horizons*, vol. 62, no. 6, pp. 751–759, Nov. 2019, doi: 10.1016/J.BUSHOR.2019.07.008.