Digital Payments in Indonesia: Understanding the Effect of Application Security on User Trust

Maheswara Rabbani¹, Juan Daniel Wijaya², Rendy Sanjaya Kusuma³, Wilhelmus Billion Pius Purba⁴, Robert Marchelino Tajib⁵

¹maheswara.rabbani@binus.ac.id, ²juan.wijaya001@binus.ac.id, ³rendy.kusuma@binus.ac.id, ⁴wilhelmus.purba@binus.ac.id, ⁵robert.tajib001@binus.ac.id

¹,²,³,⁴,⁵Information Systems Department, BINUS Graduate Program - Master in Information System Management, Bina Nusantara University, Jakarta, Indonesia, 11480

Article Information
Submitted: 8 Oct 2023
Reviewed: 17 Oct 2023
Accepted: 30 Oct 2023

Abstract
Technological developments present digital payment innovations for fast and practical transaction processes. Many digital wallets (e-wallet) services have emerged recently, becoming a trend in Indonesia. However, digital payments carry the risk of hacking user accounts, fraud (scams), phishing, and other criminal acts that aim to steal users' personal information. Financial is a sensitive issue; security is essential to digital payments. The research aims to analyze the effect of application security on user trust when making online transactions using digital payment applications. The study used a descriptive statistical method by distributing questionnaires to 50 Indonesians who have made electronic payments at least once for transactions. The study results show that application security significantly affects user trust in digital payments. Research results from various references show that application security influences impulse buying behavior and intentions to use e-wallet platforms.
A. Introduction

Technological developments in the world have changed people’s lifestyles. Nowadays, everyone who uses technology can send and receive information very quickly. The impact felt by the community is the ease, speed, and efficiency of a process [1]. The internet, one of the information technologies, has been used for various purposes, including buying and selling transactions [2].

Digitalization presents innovations that allow payments to be made using various online methods [3]. Many digital wallets (e-wallet) services have emerged recently, becoming a trend in Indonesia [4]. Online payment methods are considered beneficial because they are fast and practical [5]. The payment system connected directly to the smartphone via the internet makes it fast and functional.

Technological progress is not always positive but has harmful risks that must be considered. Behind the convenience and advantages of digital payment methods, security is a crucial aspect in this case because it involves personal, financial, and other sensitive data [6]. Many people are currently irresponsible in using technology, making it a loophole for committing crimes [7]. Some of the cybercrime phenomena that are happening today are hacking of user accounts, fraud (scams), phishing, and other criminal acts that aim to steal users’ personal information [8]. Personal data such as user identity, financial balances, credit cards, and information recorded on a system risk being misused by these irresponsible persons [6] [9].

This issue is crucial for business owners to pay attention to from digital payments because one’s finances are sensitive. Digital payments should be made as safe as possible so that users can avoid crime or unwanted things. However, a company must maintain user satisfaction for business continuity. Based on this background, the following problem formulation arises:

1. Does application security significantly affect user trust in digital payments?
2. What are the characteristics and behavior of users when using online digital payments as a transaction method?

From the formulation of the problem, this research is limited by security and user trust in digital payment applications in Indonesia. The research aims to analyze the effect of application security on user trust when making online transactions using digital payment applications. That way, the results of this study are likely helpful as a theoretical basis or reference for subsequent research. In addition, research is also beneficial for individuals, organizations, or companies to understand the effect of security on user trust in digital payment systems.

B. Research Method

1. Research Model

This study utilizes a quantitative approach, and the analysis method used is descriptive statistical analysis. Descriptive statistics are used to compile, process, analyze, and present numerical data obtained or collected to provide a clear picture and description of a phenomenon, event, or situation [10]. The reason for using this method is because this method is the most suitable for knowing community behavior patterns. This study also conducts hypothesis testing to determine the level of security of electronic payment applications circulating in Indonesia based on the level of user trust in e-payment applications.
2. Research Variables
In this study, one independent variable and one dependent variable will be used, which will serve to determine the security level of electronic payment applications in Indonesia. Independent variables are variables that play a role in influencing other variables. In contrast, the dependent variable is a variable that is used as a factor that is affected by one or several other variables [11]. From this explanation, the variables in this study are:
  a. Variable X (independent variable), namely application security.
  b. Variable Y (dependent variable), namely user trust in digital payments.

3. Variable Measurement
In conducting research, trials are needed in the affective domain [12]. This study uses a Likert scale to calculate the weight in each category. The Likert scale is commonly used in questionnaires and is the most widely used scale for research [13]. The categories used on the Likert scale in this study are:
   1. SD (Strongly Disagree)
   2. D (Disagree)
   3. N (Neutral)
   4. A (Agree)
   5. SA (Strongly Agree)

4. Hypothesis
This study aims to prove the hypothesis that security affects the level of user trust in digital payments. The hypothesis can be interpreted as an initial conjecture that is temporary or can also be referred to as an opinion that still needs to be proven true [14]. There are two hypotheses determined, namely H0 and HA:
   • H0: Application security does not significantly affect user trust in digital payments.
   • HA: Application security significantly affects user trust in digital payments.

5. Population and Sample
The population is all research subjects in a research area. The research subjects are a collection of individuals or objects that have certain qualities and characteristics. Quality and characteristics are determined in research to study the nature of the population concerned, and then conclusions are drawn [15]. Based on this explanation, the population in this study is Indonesian people who use electronic or digital payments for transactions.

The sample is part or representative of the population to be studied. The sample must be ensured that it correctly represents the population in order to get valid results when taking measurements [15]. This study took a sample of 50 Indonesians who have made electronic payments at least once for transactions.

6. Research Instrument Testing
A research instrument is a tool used to measure an object measuring. In addition, the research instrument also means the collection of data regarding a variable [16]. This study uses a questionnaire as an instrument. Questionnaires in a
Google Form will be distributed online via social media. The indicators for each variable are described in Table 1.

**Table 1. Research Variables and Indicators**

<table>
<thead>
<tr>
<th>Variable</th>
<th>No.</th>
<th>indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security (X)</td>
<td>1</td>
<td>Digital payment applications are safe to use</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Digital payments do not pose financial and user privacy concerns</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>In my opinion, application security is important</td>
</tr>
<tr>
<td>User Trust in Digital Payments (Y)</td>
<td>4</td>
<td>Digital payment apps can be trusted to use</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Satisfied with application security because it meets expectations</td>
</tr>
</tbody>
</table>

C. Result and Discussion

1. Result

In this study, a sample of 50 digital payment users was taken. Each respondent was given a questionnaire to provide answers to the statements provided. To identify respondent profiles, it is necessary to describe the characteristics of the respondents in this study. The following are the characteristics of the respondents:

![Respondents' Characteristics by Age](image)

**Figure 1. Respondents' Characteristics by Age**

Figure 1 shows that respondents dominated the study with an age range between 18-25 years. In this study, respondents aged 18-25 years amounted to 41 people or 82%, aged <17 years amounted to four people or 8%, aged 26-35 years amounted to two people or 4%, and 36-50 years amounted to three people or 6%.
Figure 2. Respondents' Characteristics by Occupation

Figure 2 shows that this research is dominated by respondents who work as a student. In this study, respondents who work as students are 40 people or 80%, respondents who work as employees are four people or 8%, respondents who are online store sellers are one person or 2%, respondents who work as entrepreneurs are four people or 8%, and respondents who have other activities amount to one person or 2%.

Figure 3. Respondents' Characteristics by Income

Figure 3 shows that this research is dominated by respondents with an income of less than IDR 1,000,000. In this study, respondents with an income range of <IDR 1,000,000 totaled 31 people or 62%, respondents with an income range of IDR 1,000,000 - 3,999,999 totaled 14 people or 28%, respondents with an income range of IDR 4,000,000 - 9,999,999 totaled five people or 10%, and there were no respondents who earned >Rp 10,000,000 (0%).
Figure 4 shows that this research is dominated by respondents who use OVO as a digital payment option with an e-wallet. In this study, 29 respondents, or 58\%, used OVO as their payment method, while 21 respondents, or 42\%, used ShopeePay as their payment method. The questionnaire results in this statement show that between OVO and ShopeePay, the OVO e-wallet is more widely used by Indonesians.

Figure 5 shows that this research is dominated by respondents who top up an e-wallet balance of IDR 50,000 - 199,000 in one transaction. In this study, respondents with a top-up balance of IDR 50,000 - 199,000 totaled 25 people or 50\%, respondents with a top-up balance of < IDR 50,000 totaled five people or 10\%, respondents with a top-up balance of IDR 200,000 - 499,000 amounted to 12 people or 24\%, and respondents with a top-up balance of IDR 500,000 - 1,000,000 amounted to eight people or 16\%. The results of the questionnaire in this statement show that most Indonesian people top up balances of IDR 50,000 - 199,000 in one transaction.
1.1 Validity Test

A validity test is a measure that shows the level of validity of the instrument used in research. An instrument can be valid if it is precise and appropriate to answer carefully about the variable to be measured [17]. The convergent validity test was carried out in this study to see the loading factor value of each indicator on the variable. A loading factor of 0.5 or more is considered to have strong enough validation to explain latent variables [18] [19].

![Figure 6. Model Validity Test Results](image)

Figure 6 shows the results of testing the model’s validity using the SmartPLS tool. In this study, the minimum acceptable loading factor limit is 0.5. Based on the analysis results in the figure above, all indicators have a loading factor above 0.5, so the indicators are declared valid because they meet the convergent validity requirements.

1.2 Reliability Test

In addition to validity, a good measuring tool must also be reliable. Reliability is a measurement tool to show the extent to which an instrument can be trusted or relied upon. A good instrument is an instrument that gets the same results or remains consistent when used for repeated measurements. A good measuring tool is not only valid but also reliable [17]. Figure 7 shows the results of the model reliability test.

![Figure 7. Model Reliability Test Results](image)

Reliability can be assessed from the value of Cronbach’s Alpha and Composite Reliability of each variable. The recommended Cronbach’s Alpha and Composite Reliability values are more than 0.7 [19]. Based on the results of the reliability test in Figure 7, the composite Cronbach’s Alpha and Composite Reliability values were obtained > 0.7. In conclusion, all variables are declared reliable because they meet the reliability requirements.

1.3 Hypothesis Testing

Hypothesis testing aims to prove the hypothesis about the relationship between application security and user trust in digital payments. This test was
carried out using the SmartPLS tool. The following are the requirements of the hypothesis in this study [20]:

- $H_0$: $P$-Value > 0.05
- $H_A$: $P$-Value < 0.05

**Figure 8. PLS Path Analysis Results (P Values)**

Figure 8 shows a result that there is a relationship between application security and user trust in digital payments. The significance value ($P$-Value) is 0.00, where the $P$-Value is less than 0.05. If the $P$-Value is less than the significance level (0.05), $H_0$ is rejected, and $H_A$ is accepted [21]. From these results, it can be concluded that application security significantly affects user trust in digital payments.

1.4 Descriptive Statistics

The research variables are divided into 2 with the results of each calculation. Based on the research that has been done, the following data results are obtained:

<table>
<thead>
<tr>
<th>Variable</th>
<th>X</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>12</td>
<td>8</td>
</tr>
<tr>
<td><strong>Mean</strong></td>
<td>12.58</td>
<td>8.54</td>
</tr>
<tr>
<td><strong>Skewness</strong></td>
<td>-0.113</td>
<td>0.177</td>
</tr>
<tr>
<td><strong>Kurtosis</strong></td>
<td>-0.928</td>
<td>-0.904</td>
</tr>
<tr>
<td><strong>Max</strong></td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td><strong>Min</strong></td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td><strong>Variance</strong></td>
<td>3.269</td>
<td>0.907</td>
</tr>
<tr>
<td><strong>Standard Deviation</strong></td>
<td>1.808</td>
<td>0.952</td>
</tr>
<tr>
<td><strong>Median</strong></td>
<td>12</td>
<td>8</td>
</tr>
</tbody>
</table>

Variable $X$, namely application security, has a calculation with the result: mean has a value of 12.58, and for mode, it has a value of 12. Skewness has a value of -0.113, while kurtosis has a value of -0.928. The maximum and minimum values are 15 and 9, respectively, resulting in a range of 6. The variance is at 3.269, the standard deviation is 1.808, and the median is 12.

As for the calculation of the $Y$ variable, namely the user trust in digital payments variable, it has a calculation with the result: the mean has a value of 8.54. For mode, a score of 8 is obtained. For skewness, it is at 0.177, while kurtosis is at -0.904. The maximum and minimum values are 10 and 7, respectively, resulting in a range of 3. For a variance value of 0.907, the standard deviation is 0.952, and the median is 8.
2. Discussion

This section explains further the results of the research conducted by distributing questionnaires to 50 respondents with the criteria of Indonesians who have made electronic payments at least once for transactions.

The initial hypothesis of the study is that there is an effect of application security on the use of digital payments. After going through hypothesis testing, the results show that application security significantly affects user trust in digital payments. This is proven by calculating the P-Value using the SmartPLS tool. The results of hypothesis testing show that H0 is rejected, and HA is accepted. The safer the security level of an application, the more trusted users will be in using the application as a digital payment option.

Mala Kresiana Utami (2021) [22] researched trust, usability, and security on interest in using the Linkaja mobile payment (e-wallet). The results show that security, trust, and convenience positively and significantly affect interest in using Linkaja mobile payment. Another study conducted by Adela Rossa and Fathir Ashfath (2022) [23] revealed that security and trust influence impulse buying behavior toward SPaylater (e-wallet) users. Security features such as biometric verification and OTP codes generate a perception of security and trust. Because of this, users are increasingly using SPaylater as their payment method for e-commerce transactions. To prove that user trust in a digital payment application is important, research by Nopy Ernawati and Lina Noersanti (2020) [24] also reveals that the trust variable significantly influences interest in using the OVO (e-wallet) application.

This research simultaneously supports statements from previous research results regarding security and trust in using digital payment applications. However, in previous research, the variables of security and trust were used as independent variables that influenced the variables of interest in using applications or impulse buying behavior. The novelty of this research is to consider whether application security directly affects user trust in using digital payments. Application security is the independent variable, while user trust in digital payments is the dependent variable. Because application security significantly affects user trust in digital payments, digital payment applications must increase user perceptions of trust by increasing application security. Suppose the user feels the application is safe. In that case, a sense of trust will be created in a product or service so that the user will use the application repeatedly without worrying about security breaches [23].

D. Conclusion

Based on the results of research between application security relationships and user trust in digital payments, the following conclusions can be drawn:

1. Application security significantly affects user trust in digital payments. This means that the security of digital payment applications, especially e-wallets, is an essential aspect for users when considering using applications as a means of payment for transactions. In addition, application security positively impacts users so that they can enjoy the services offered as a means of payment that is safe and useful.
2. User trust in e-wallets or digital payments has a significant influence on financial transactions, especially e-commerce. This means that user trust positively impacts e-commerce companies or e-wallet companies.

With technological advances increasing rapidly, security is an important thing that must be considered; security is an aspect that determines trust. Start-ups, e-commerce companies, and digital payment applications must innovate more in their digital payment implementation and security design. One of them is with technological advances that use fingerprint or face ID biometrics for verification before making digital payments. There are still many examples or other methods, each of which has positive and negative sides that must be considered because it will impact the community’s future payment needs.

E. References


