Journal of Economics and Social Sciences (JESS)
Vol. 4, 1 (January-June, 2025), pp. 407-418
EISSN: 2808-5094, DOI: 10.59525/jess.v4i1.757

The influence of CyberCrime on the level of trust of users of Ewallet products in Mobile Banking Services reviewed Islamic Economic Perspective (user study of UIN RIL student Fund E-Wallet application)

Rilo Abdi Pramestu[1], Muhammad Kurniawan[2], Agus Kurniawan[3]

[1] UIN Raden Intan Lampung, Indonesia; riloabdipra@gmail.com
[2] UIN Raden Intan Lampung, Indonesia; muhammadkurniawan@radenintan.ac.id
[3] UIN Raden Intan Lampung, Indonesia; Aguskurniawan@radenintan.ac.id

ARTICLE INFO

Keywords:

Cyber crime;
consumer trust;
e-wallet;
mobile banking;
Islamic economics;
Fund application

Article history:

Received 2025-04-20
Revised 2025-05-22
Accepted 2025-07-13

ABSTRACT

The development of financial technology, especially mobile banking services and e-wallet applications, increasingly provides convenience in digital transactions. However, the increasing incidence of cyber crime (cyber crime) poses serious problems related to user confidence in the security of the service. This study aims to analyze the influence of cyber crime on the level of confidence of e-wallet users in mobile banking services in the perspective of Islamic economics. With quantitative methods and survey approaches to student users of the Dana e-wallet application at UIN RIL, the results of the study show that cyber crime has a positive influence on user trust. The Islamic economic perspective emphasizes the importance of Amanah and adil in maintaining trust so that digital transactions remain halal and reliable. This study recommends improving security, educating users, and implementing sharia principles in e-wallet services.

Corresponding Author:
Rilo Abdi Pramestu
UIN Raden Intan Lampung, Indonesia; riloabdipra@gmail.com

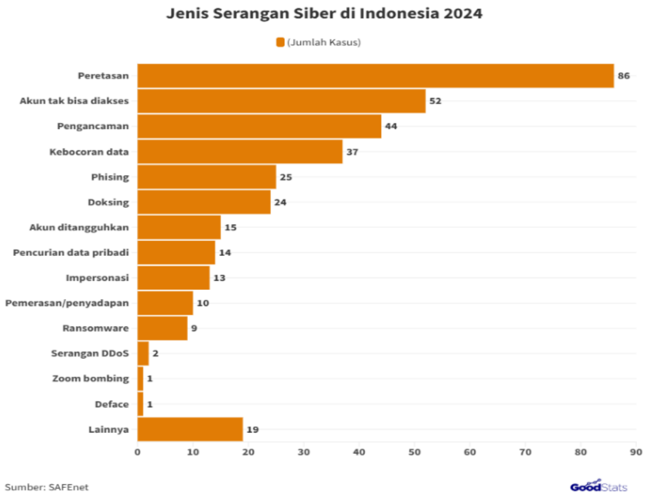
1. INTRODUCTION

In this era of globalization, everything happens all the time. A widespread process that makes it impossible for society to avoid. The cultural norms and practices of modern Indonesian society have evolved in response to globalization. Communication is just one of the areas that has benefited from the technical advances brought by globalization (Antonio, 2018). Human beings engage in communication as one of their fundamental life activities. A person's relationship with other individuals is always there because they are social beings. Every aspect of life, both external and internal, arouses insatiable human curiosity. Humans have an innate need to know more about the world around them and the people in it (Amelia, Fadilla, & Aravik, 2025)

The rapid development of Information Technology has brought significant changes in the digital payment system. E-wallet applications such as DANA, OVO, and GoPay are the top choices for people because of the speed, convenience, and efficiency in transactions (Handayani & Soeparan, 2022).

However, behind this ease comes a serious threat, namely cyber crime. The rapid development of digital-based financial services, especially mobile banking and e-wallet applications, has changed the way modern society transacts. Students as active users of this technology also utilize e-wallet applications for various daily financial needs, such as college payments,credit purchases, and other needs. However, amid these facilities, security risks arise, especially cyber crimes such as phishing, data theft,and digital fraud that have the potential to reduce the level of user trust (Anjeli, Putri, Perengki, & Soleh, 2025).

Figure 1. Cyber Crime in Indonesia



Sources: GoodStats, 2025.

Cyber attacks have evolved along with the development of communication and Information Technology. In the past, words like "hacker" or "cracker" denoted a person with special skills who gained access to a computer system. There are many systems and technologies out there that can infiltrate other systems and harm them (Habibi & Liviani, 2020).

According to the Organization of Community Development (OECD) cyber crime is a form of illegal access to data transmission. Cyber crime is a cyber activity that utilizes computer technology as the main tool of crime. The influence of rapidly growing technological advances that lead to increased cases of cyber crime. This is inseparable from the emergence of an increasing growth of internert users and resulting in a lot of internet crime in Indonesia (Nupus, 2025). Cyber crime is an act of crime committed over the internet, with the aim of damaging or obtaining unauthorized access to data or computer systems.

The level of user trust in digital services, such as e-wallets, is a crucial factor that influences usage decisions and user loyalty. In this context, trust can be defined as a user's belief that a digital service will operate reliably, securely, and in accordance with their expectations (Djatmiko, Halim, & Hellyani, 2024). In the perspective of Islamic economics, trust (amanah) is a fundamental value that must be maintained in every transaction. This trust includes the belief that the service provider will perform its functions honestly and fairly, and protect the rights of users in accordance with Sharia principles.

Users ' trust in e-wallet services in mobile banking is increasingly eroded due to the rise of cyber crime cases such as data theft, phishing, and account hacking that cause financial losses for consumers (Sari & Fitri, 2025). This digital security threat makes some users hesitant to continue using e-wallet services, including The Dana application, which is popular among UIN Raden Intan Lampung students. In the context of Islamic economics, trust (tsiqah) becomes a fundamental element in financial transactions, because it involves the principles of honesty, transparency, and security. When this aspect is disrupted by cybercrime, it is indirectly contrary to the values of maqashid Sharia, especially in terms of property protection (hifzh al-mal). Therefore, it is important to examine the extent to which cyber crime affects the level of trust of e-wallet users from the perspective of Islamic economics. However, there are not many studies that specifically examine the impact of cyber crime on the trust of e-wallet users in the frame of Islamic economic values, especially among student users of the Dana application at UIN Raden Intan Lampung.

This study aims to assess the influence of cyber crime on the level of confidence of users of e-wallet products in mobile banking services, with a focus on users of Dana applications among UIN Raden Intan Lampung students. In the context of Islamic economics, trust becomes the main foundation in every financial transaction because it is closely related to the principles of honesty, responsibility, and protection of property. Therefore, this study is explicitly directed to answer how the form and level of user trust in the Dana e-wallet application in the midst of the rise of cyber crime cases, the extent to which cybercrime affects this trust, and how the Islamic economic perspective views the phenomenon. Thus, the study not only provides an empirical picture of the relationship between cyber crime and user trust, but also offers a relevant Islamic values-based viewpoint in the development of a secure and ethical digital financial system.

2. METHODS

Types and approaches of research

This research is a quantitative research with associative approach. This approach is used to determine and analyze the influence of cyber crime on the level of confidence of users of e-wallet products in mobile banking services, viewed from the perspective of Islamic economics.

Population and sample

The population in this study is all UIN Raden Intan Lampung students who use the DANA application as an e-wallet. However, because there is no exact data on the number of active users of DANA among UIN RIL students, the population is considered to be an infinite population.

Sampling techniques using purposive sampling techniques, namely sampling techniques with certain considerations or criteria that are relevant to the purpose of the study. The criteria of respondents in this study include: (1) active students of UIN RIL, (2) have used the DANA e-wallet application for at least the last three months. Data collection techniques are using questionnaires and documentation to support secondary data and research background.

Frame Of Mind

Based on the research background, the formulation of the problems that have been discussed regarding the influence of cyber crimer on the level of user trust. And whether cyber crime has a relationship to the level of user trust when associated with an Islamic economic perspective. So the conceptual framework as follows:

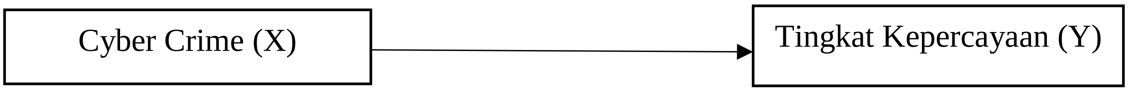


Figure 1. Frame Of Mind

Hypothesis

H1: Cyber Crime has a positive effect on the confidence level of E-wallets

Data Analysis Techniques

The data analysis technique in this study uses Partial Least Square (PLS) approach, which is operated through SmartPLS software version 4. Structural Equation Modeling (SEM) is a set of statistical techniques that allow testing a series of relatively complex relationships that cannot be solved by linear regression equations (Harahap, 2020). PLS was chosen because it is suitable for the analysis of casual relationships between latent variables measured through manifest indicators, as well as suitable for small to medium sample sizes and data that do not have to be normally distributed.

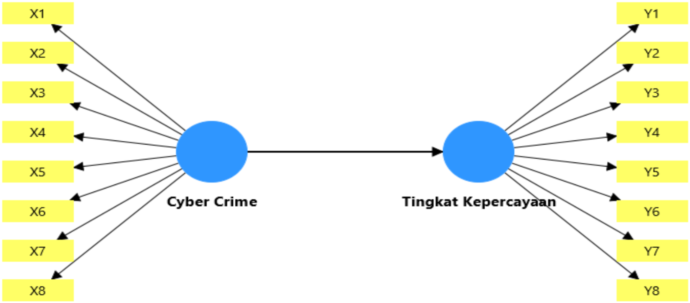


Figure 2. Partial Least Square Model Scheme
Source: processed Data Smart PLS 4 (2025)

3. FINDINGS AND DISCUSSION

Measurement Model (Outer Model)

The Outer model in Partial Least Squares Structural Equation Modeling (PLS-SEM) is an important part that explains the relationship between latent constructs and their measuring indicators. There are two types of outer models, namely reflective and formative, each of which has different characteristics and theoretical implications. Evaluation of the outer model is done to ensure that the construct is measured in a valid and reliable manner, using criteria such as convergent validity (AVE ≥ 0.50), discriminant validity (Fornell-Larcker and HTMT), and internal reliability (Composite Reliability and Cronbach's Alpha ≥ 0.70).

Proper application and evaluation of the outer model is very important so that the results of the analysis in the structural model can be interpreted accurately and can be accounted for. Based on the latest literature and journals, it can be concluded that a good understanding of the outer model is the main key in building a strong measurement model and supporting the overall validity of PLS-SEM-based research (Mariani, Suryani, Saufi, & Soesetio, 2024).

The outer model image can be seen in Figure 3. Below.

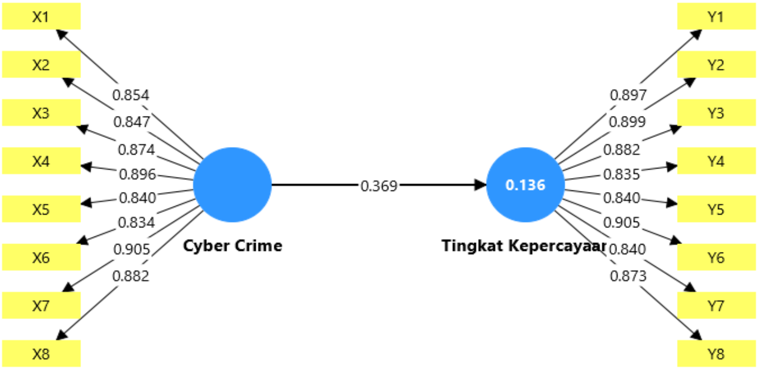


Figure 3. Measurement model Phase II (Outer Model)
Source: Smartpls 4 Processed Data (2025)

Test Of Convergent Validity

Convergent validity is an important aspect in the evaluation of measurement models in Partial Least Squares Structural Equation Modeling (PLS-SEM). This validity indicates to what extent the indicators that are supposed to measure the same construct are really highly correlated with each other (Sofyani, 2025). Theoretically, convergent validity can be evaluated through two main components, namely the value of average Variance Extracted (Ave), which is ideally 0.50, and the value of loading factor indicator, which should be 0.70 (Hair & Alamer, 2022).

Outer loading is a coefficient that shows how strong the relationship between indicators (measurable variables) and latent constructs (variables that cannot be measured directly) in reflective measurement models in Partial Least Squares Structural Equation Modeling (PLS-SEM) (Sholihin & Ratmono, 2021). A high outer loading value indicates that the indicator is a good representation of the latent construct it measures (Dwiputri, 2019). Here are the results of the outer loading test in Table 1.

Table 1. Outer Loading Test Results

Variable	Indicator	Outer Loading	Conclusion
Cyber Crime (X)	X1	0.854	Valid
	X2	0.847	Valid
	X3	0.874	Valid
	X4	0.896	Valid
	X5	0.840	Valid
	X6	0.834	Valid
	X7	0.905	Valid
	X8	0.882	Valid
User Trust Level (Y)	Y1	0.897	Valid
	Y2	0.899	Valid
	Y3	0.882	Valid
	Y4	0.835	Valid
	Y5	0.840	Valid
	Y6	0.905	Valid
	Y7	0.840	Valid
	Y8	0.873	Valid

Source: Smartpls Processed Data 4 (2025)

Based on the results of PLS-SEM analysis, all indicators in the measurement model have an outer loading value above 0.70, which indicates that these indicators are valid and able to reflect the latent construct they measure consistently. The outer loading value that meets this threshold also indicates that each indicator has a significant contribution in explaining the latent variables, so it can be concluded that the measurement model has met the convergent validity requirement.

Average Variance Extracted (AVE)

Average Variance Extracted (AVE) is a measure used to assess convergent validity in reflective measurement models in Partial Least Squares Structural Equation Modeling (PLS-SEM). AVE measures the extent to which latent constructs explain the variance of its indicators (Sofyani, 2025).

According to (Safaria, Rahayu, & Rahaju, 2024), the high value of AVE indicates that the construct is able to explain most of the variance of its indicators, which indicates good convergent validity. In general, the value of Ave α 0.50 is considered adequate, since it indicates that the latent construct explains at least 50% of the variance of its indicators. If the Ave value is below 0.50, this may indicate that the construct may not adequately explain the variance of the indicators, so convergent validity needs to be evaluated further. Here is the value of Ave inthis study:

Tabel 2. Ave value test results

Variabel	Average Variance exracted (AVE)
Cyber Crime (X)	0.751
Tingkat Kepercayaan (Y)	0.760

Source: Smartpls Processed Data 4 (2025)

Based on the results of the analysis of measurement models with PLS-SEM approach, the average Variance Extracted (AVE) for Cyber Crime and user trust variables above 0.50. This indicates that both constructs have met the criterion of convergent validity, where more than 50% of the variance of their indicators can be explained by the latent construct. Thus, the indicators used in measuring Cyber Crime and user trust were found to be valid in a convergent manner and worthy of use in this research model.

Discriminant Validity Test

Discriminant validity is one of the important aspects in evaluating the quality of measurement model in Partial Least Squares Structural Equation Modeling (PLS-SEM) method. This validity indicates the extent to which a construct really differs from other constructs in the same model, both theoretically and empirically (Ramadhan et al., 2025).

In other words, discriminant validity ensures that the indicators of a construct do not have a high correlation with other constructs, so that each construct is able to measure a unique concept (Hair & Alamer, 2022). However, a more current and recommended approach in recent studies is the Heterotrait-Monotrait Ratio (HTMT). HTMT is a correlation ratio based method that is considered more sensitive and accurate in detecting discriminant validity. According to (Hair & Alamer, 2022), HTMT values that are below 0.85 or 0.90 (depending on the context of the study) indicate that the construct in the model has met the discriminant validity criteria.

Table 3. Test results with HTMT

	Cyber Crime	Confidence Level
Cyber Crime		
Confidence Level	0.367	

Source: SmartPLS processed Data 4 (2025)

The results showed that the value of Heterotrait-Monotrait Ratio (HTMT) between constructs was 0.367, which is below the threshold of 0.85. This indicates that the discriminant validity between constructs has been adequately met. Thus, each construct in the model can be said to be significantly different, so the measurement model is worth using for further analysis.

Reliability Test

Reliability is a measure of the consistency of a construct in measuring the variables represented by its indicators. In the analysis of Partial Least Squares Structural Equation Modeling (PLS-SEM), reliability is usually measured using Cronbach's Alpha and Composite Reliability (CR). Cronbach's Alpha measures internal consistency between indicators, with an ideal value of at least 0.70(Putu, Dewi, Made, & Wibawa, 2023).

However, Composite Reliability is more recommended because it can consider the weight of different indicators so as to provide a more accurate estimate of reliability (Sholihin & Ratmono, 2021). A good CR value should also reach a minimum of 0.70, which indicates that the construct is measured consistently and reliably. Thus, reliability testing becomes an important step in ensuring that research instruments are able to produce valid and consistent data.

Table 4. Reliability Test Results

Variable	Cronbach's Alpha	*Composite Reliability* (rho_c)	Conclusion
Cyber Crime (X)	0.953	0.960	Reliabel
Confidence Level (Y)	0.955	0.962	Reliabel

Source: processed Data SmartPLS 4 (2025)

Based on the results of reliability testing using Cronbach's Alpha and Composite Reliability (CR), all constructs in this study showed values above 0.70. The value indicates that the indicators in each construct have sufficient internal consistency and can be trusted to measure the variable in question. In other words, this research instrument meets good reliability criteria so that the data obtained are valid for further analysis and produce scientifically accountable conclusions.

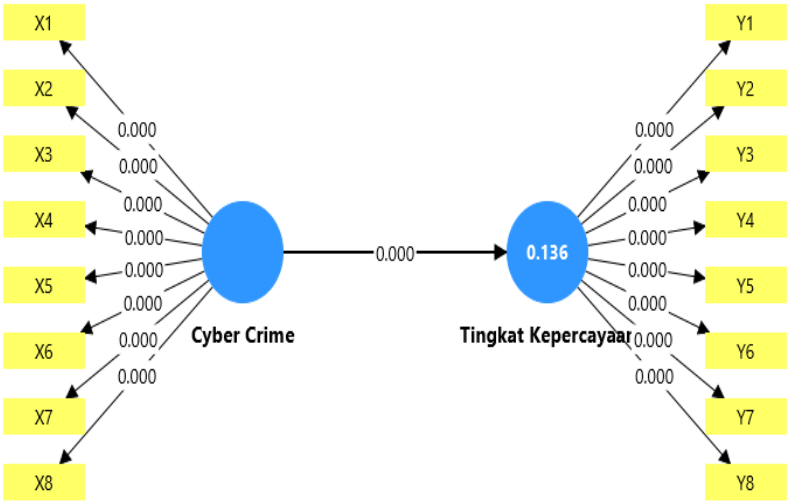
Structural Model (Inner Model)

Inner model or structural model in Partial Least Squares Structural Equation Modeling (PLS-SEM) plays a role in explaining the relationship between latent constructs based on previously formulated hypotheses. The Inner model describes the direction and strength of the influence of exogenous constructs on endogenous constructs in the model. Evaluation of the inner model aims to assess whether the causal relationships between constructs are in accordance with the theory and empirical data used (Sholiha & Salamah, 2016).

According to Hair et al. (2022), the evaluation of the inner model in PLS-SEM involves several key indicators. First, multicollinearity Test between constructs is done by using Variance Inflation Factor (VIF) value, where the value below 5 indicates that there is no multicollinearity problem. Second, path coefficients were analyzed to determine the direction and magnitude of influence between constructs, which were then tested for significance through bootstrapping methods. Third, the value of R2 (R-squared) is used to measure the level of ability of exogenous constructs in explaining the variance of endogenous constructs. A higher R2 value indicates the model has strong apparent power.

Furthermore, the F2 effect size was used to assess the contribution of each exogenous construct to the endogenous construct, with criteria of 0.02 (small), 0.15 (medium), and 0.35 (large). Finally, the value of Q2 (predictive relevance) obtained through the blindfolding technique is used to assess the predictive ability of the model; a value of Q2 > 0 indicates the presence of predictive relevance.

The inner model bias seen in the picture below.



Source: Smartpls 4 Processed Data (2025)

Figure 4. Phase II Measurement Model (Inner Model)

Collinearity Variance Inflation factor (VIF)

Variance Inflation Factor (VIF) is one of the statistical indicators used to detect the presence of multicollinearity between independent variables in a regression model or structural model such as SEM-PLS (Structural Equation Modeling - Partial Least Squares). Multicollinearity occurs when two or more independent variables are highly correlated with each other, which can lead to instability in parameter estimation and decrease model validity (Hair & Alamer, 2022).

Mathematically, VIF is calculated based on the inverse of the value of the coefficient of determination (R2) of the regression results of each independent variable to other independent variables. A high VIF value indicates that a variable has a strong correlation with other variables, which indicates the presence of multicollinearity. In practice, a value of VIF < 5 is still acceptable, but some literature suggests a stricter limit of VIF < 3.3 for more conservative and accurate results (Harahap, 2020)

Table 5. VIF test results

Variabel	Indicator	VIF
Cyber Crime (X)	X1	3.018
	X2	3.195
	X3	3.400
	X4	4.399
	X5	2.895
	X6	3.453
	X7	4.394
	X8	4.118
User Trust Level (Y)	Y1	4.386
	Y2	4.192
	Y3	4.059
	Y4	2.989
	Y5	3.230
	Y6	4.646
	Y7	3.042
	Y8	3.496

Source: processed Data SmartPLS 4 (2025)

Multicollinearity test results shown in Table 5 show that all Variance Inflation Factor (VIF) values are below 5. This indicates that there is no multicollinearity between indicators in the model, so that each variable is free from high correlation with each other. Thus, this research model satisfies the assumption of free multicollinearity and can proceed to further stages of structural analysis with stable and valid estimates.

R-Square (R2)

R-Square (R2) or coefficient of determination is a statistical measure that shows how much the independent variable is able to account for the dependent variable in a model. In both regression and PLS-SEM Analyses, R2 values ranged from 0 to 1, where values close to 1 indicated high predictive ability (Hair et al., 2022).

According to Sarstedt et al. (2023), the interpretation of R2 in the PLS-SEM is divided into three categories: R2 α 0.75 (strong), R2 α 0.50 (moderate), and R2 α 0.25 (weak). This value is an important indicator in assessing the feasibility of structural models, especially in quantitative research based on latent constructs. In addition, Latan (2024) suggested that R2 be analyzed along with other predictive measures such as Q2 and f2 to obtain a more comprehensive picture.

Table 6. R-Square

Item	R-square	R-square adjusted
User Trust Level (Y)	0.136	0.128

Source: SmartPLS 4 processed data (2025)

The R-Square value of 0.128 indicates that the model is only able to explain 12.8% of the variance of the dependent variable, which indicates that the predictive power of the model is still relatively low. Nonetheless, in exploratory research or fields with complex variables, low R2 values are still acceptable as long as they are supported by other analyses such as the validity and significance of relationships between variables (Hair & Alamer, 2022)

F-Square

f-square (f2) is an effect size used in structural model analysis, especially in Partial Least Squares Structural Equation Modeling (PLS-SEM). This measure measures how much an independent variable contributes to the variance of the dependent variable in the model. The value of f2 is calculated by comparing the value of R-Square (R2) in a model that includes a certain independent variable with a model that does not include it. The greater the value of f2, the greater the effect of the variable on the dependent variable.

According to Cohen (1988), the interpretation of the value of f2 can be divided into three categories, namely the small effect if f2 ⩾ 0.02, medium effect if f2 ⩾ 0.15, and large effect if f2 ⩾ 0.35. This measure becomes important in the evaluation of the PLS-SEM model to assess the significance and strength of the influence of the independent variable individually on the dependent variable (Hair & Alamer, 2022)

Table 7. F-Square test result

Konstruk	f-Square	Description
X1-> Y	0.158	Medium

Source: SmartPLS 4 Processed Data (2025)

Based on the results of the analysis in Table 7, obtained F-square value of 0.158, which indicates that the independent variable gives a moderate effect on the dependent variable in the model. This value indicates a significant contribution, so that the variable has an important role in explaining changes in the variance of the dependent variable.

Hypothesis Test

Hypothesis testing in SmartPLS is done by testing the path coefficients and their significance using bootstrapping techniques. Bootstrapping generates statistical t-values and p-values to determine whether the relationship between variables is significant. Generally, values of t > 1.96 and p < 0.05 indicate an accepted hypothesis (Hair & Alamer, 2022)SmartPLS is particularly suitable for research with non-normal data and latent variable models, so it is widely used for the validation of conceptual models in the business and social fields (Ali, Rasoolimanesh, Sarstedt, Ringle, & Ryu, 2018).

Table 8. Hypothesis Test Results

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T statistics (lO/STDEVl)	P values
Cyber Crime (X) → Confidence Level (Y)	0.396	0.388	0.089	4.169	0.000

Source: smartpls 4 processed Data (2025)

Based on the results of data processing using SmartPLS 4 shown in Table 8, it is known that the Cyber Crime variable (X) has a significant influence on the level of user confidence (Y) in e-wallet products in mobile banking services. The results of the analysis showed that:

1. The value of the Original Sample (O) of 0.396 indicates a positive influence between cyber crime and the level of user trust, but the direction of this relationship needs to be interpreted contextually.

In this context, although the value is positive, it could represent the user's perception of increased security in the midst of rampant cyber crime.

2. The T-statistic value is 4,169 > 1,96, which means that the relationship between these variables is statistically significant at a 95% confidence level.
3. The P-Value of 0.000 < 0.05, which reinforces the evidence that the accepted hypothesis, namely cyber crime has a significant effect on the level of user trust.
4. Thus, it can be concluded that Cyber Crime significantly affects the level of trust of E-Wallet users. This means that threats or cyber crime events can affect user confidence in using e-wallet applications, including funds, especially among UIN RIL students.

Discussion

Based on the results of data analysis that has been done, it is known that the variable Cyber Crime (X) has a significant and positive effect on the variable level of trust of users of E-Wallet products (Y). This means that the higher the user's perception of cybercrime threats in the use of e-wallet applications, the lower their level of trust in the service.

This finding is reinforced by the value of statistical significance that shows a real relationship between the two variables. This is in line with research (Hair & Alamer, 2022), which states that perception of digital security risks, such as cyber crime, is one of the main factors that can reduce user confidence in technology-based services.

In addition, according to (Edeh, Lo, & Khojasteh, 2023), within the framework of the PLS-SEM model, security, privacy, and risk variables are often key predictors in building or undermining user confidence in digital systems, including financial applications such as e-wallets.

From the perspective of Islamic Economics, trust (tsiqah) is the main foundation in every muamalah activity, including the use of financial technology. When the risk of cybercrime is not minimized, the values of Justice, trust, and consumer protection in Sharia principles cannot be enforced optimally.

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْٓا اِذَا تَدَايَنْتُمْ بِدَيْنٍ اِلٰٓى اَجَلٍ مُّسَمًّى فَاكْتُبُوْهُۗ وَلْيَكْتُبْ بَّيْنَكُمْ كَاتِبٌۢ بِالْعَدْلِۖ وَلَا يَأْبَ كَاتِبٌ اَنْ يَّكْتُبَ كَمَا عَلَّمَهُ اللّٰهُ فَلْيَكْتُبْۚ وَلْيُمْلِلِ الَّذِيْ
عَلَيْهِ الْحَقُّ وَلْيَتَّقِ اللّٰهَ رَبَّهٗ وَلَا يَبْخَسْ مِنْهُ شَيْـًٔاۗ فَاِنْ كَانَ الَّذِيْ عَلَيْهِ الْحَقُّ سَفِيْهًا اَوْ ضَعِيْفًا اَوْ لَا يَسْتَطِيْعُ اَنْ يُّمِلَّ هُوَ فَلْيُمْلِلْ وَلِيُّهٗ بِالْعَدْلِۗ وَاسْتَشْهِدُوْا
شَهِيْدَيْنِ مِنْ رِّجَالِكُمْۚ فَاِنْ لَّمْ يَكُوْنَا رَجُلَيْنِ فَرَجُلٌ وَّامْرَاَتٰنِ مِمَّنْ تَرْضَوْنَ مِنَ الشُّهَدَۤاءِ اَنْ تَضِلَّ اِحْدٰىهُمَا فَتُذَكِّرَ اِحْدٰىهُمَا الْاُخْرٰىۗ وَلَا يَأْبَ الشُّهَدَۤاءُ
اِذَا مَا دُعُوْا ۗ وَلَا تَسْـَٔمُوْٓا اَنْ تَكْتُبُوْهُ صَغِيْرًا اَوْ كَبِيْرًا اِلٰٓى اَجَلِهٖ ۗ ذٰلِكُمْ اَقْسَطُ عِنْدَ اللّٰهِ وَاَقْوَمُ لِلشَّهَادَةِ وَاَدْنٰٓى اَلَّا تَرْتَابُوْٓا اِلَّآ اَنْ تَكُوْنَ تِجَارَةً
حَاضِرَةً تُدِيْرُوْنَهَا بَيْنَكُمْ فَلَيْسَ عَلَيْكُمْ جُنَاحٌ اَلَّا تَكْتُبُوْهَاۗ وَاَشْهِدُوْٓا اِذَا تَبَايَعْتُمْ ۖ وَلَا يُضَاۤرَّ كَاتِبٌ وَّلَا شَهِيْدٌ ەۗ وَاِنْ تَفْعَلُوْا فَاِنَّهٗ فُسُوْقٌۢ بِكُمْ ۗ وَاتَّقُوا
اللّٰهَ ۗ وَيُعَلِّمُكُمُ اللّٰهُ ۗ وَاللّٰهُ بِكُلِّ شَيْءٍ عَلِيْمٌ

> *"O you who believe! If you are in debt for a fixed period of time, write it down. And let a scribe among you write it in truth. Let not the writer refuse to write it as Allah has taught him, so let him write. And let him who is in debt dictate, and let him fear Allah, his Lord, and let him not diminish anything from it. If the debtor is one who lacks intellect or is weak, or is unable to dictate to himself, then let his guardian dictate to him in truth. And call to witness two male witnesses among you. If there are not two men, then a man and two women from among those whom you like of the witnesses, so that if one forgets, the other may remind him. And let not the witnesses refuse when called. And do not be weary of writing it down for a term, whether it be small or great. That is more just in the sight of Allah, more able to bear witness, and more likely to bring you closer to dishonesty. And take witnesses when you trade, and do not make it difficult for the writer, nor for the witness. If you do that, it is indeed evil in you. And fear Allah; he admonishes you, and Allah has full knowledge of all things."*

This paragraph emphasizes the importance of clarity, honesty, and recording in transactions, as a form of protection of the rights of the parties to the transaction. In the context of e-wallets and mobile banking, this verse affirms that security, transparency, and trust are principles that are in line with

Islamic teachings. Cyber crimes that undermine trust and create insecurity in digital transactions are contrary to the values taught in this paragraph.

Thus, e-wallet service providers such as DANA need to actively improve security systems, transparency, and digital literacy in order to build user trust in accordance with the principles in Islamic Economics

4. CONCLUSION

Based on the analysis of 100 UIN Raden Intan Lampung student respondents using the DANA e-wallet application, it can be concluded that Cyber Crime (X) has a significant effect on the level of user trust (Y). The findings suggest that perceived threats to cybercrime have a direct impact on decreasing users ' trust in e-wallet services. In the perspective of Islamic Economics, trust is an important element in maintaining the continuity of muamalah transactions. When users feel a threat to transaction security, the value of trust, fairness, and Consumer Protection cannot be fully realized. Thus, digital security is not only a technical aspect, but also ethical and Shari'ah in the digital financial system.

This study provides an important contribution in the development of literature related to digital security and consumer behavior in Islamic economics, especially on the use of e-wallet services among students. The finding that cybercrime has a significant effect on the level of user trust shows that digital security aspects not only have a technical impact, but also affect the psychological and ethical aspects of financial transactions. In the perspective of Islamic economics, these results confirm the urgency of applying the principles of honesty, responsibility, and protection of property in digital financial services. Thus, this research not only enriches theoretical studies, but also provides a basis for policy makers and service providers to build systems that are more secure, reliable, and in accordance with Sharia values.

Based on the findings that cyber crime has a significant effect on the level of trust of Dana e-wallet application users, it is recommended that e-wallet service providers and related institutions improve digital security systems on an ongoing basis and conduct intensive education to users about preventive measures against cyber crime. In addition, the application of Islamic economic principles such as transparency (shiddiq), responsibility (amanah), and protection of property (hifzh al-mal) needs to be integrated into digital policies and services to rebuild consumer trust. Researchers are further advised to expand the variables studied, such as the influence of digital literacy or Sharia regulation on user trust, as well as conduct comparative studies between various e-wallet platforms in the context of Islamic economics.

REFERENCES

Ali, F., Rasoolimanesh, S. M., Sarstedt, M., Ringle, C. M., & Ryu, K. (2018). An assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. *International Journal of Contemporary Hospitality Management*, *30*(1), 514–538.

Amelia, K., Fadilla, F., & Aravik, H. (2025). Pengaruh Cyber Crime Terhadap Tingkat Kepercayaan Nasabah Pengguna Internet Banking (Studi Kasus Nasabah BRI A Rivai Palembang). *Jurnal Ilmiah Mahasiswa Perbankan Syariah (JIMPA)*, *5*(1), 369–376.

Anjeli, R., Putri, D. C. S., Perengki, M., & Soleh, E. (2025). *Penggunaan Cashless Di Lingkungan Mahasiswa*. Bandung: Penerbit Widina.

Antonio, T. H. D. M. R. (2018). *Journal of cybersecurity and privacy*. *1*(1), 5–8.

Djatmiko, P. N., Halim, S. W., & Hellyani, A. (2024). *Pengaruh Kemudahan Penggunaan dan Manfaat terhadap Minat Penggunaan Aplikasi E-Wallet keuntungan memengaruhi keinginan untuk menggunakan e-wallet . Penulis berharap*. *4*, 264–270.

Dwiputri, R. M. (2019). Pengaruh Tata Kelola Perusahaan Terhadap Kinerja Keuangan dan Kinerja Saham pada Indeks Saham LQ45. *Jurnal Ekonomi Dan Industri*, *20*(1).

Edeh, E., Lo, W.-J., & Khojasteh, J. (2023). Review of Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook. In *Structural Equation Modeling: A Multidisciplinary Journal* (Vol.

30). https://doi.org/10.1080/10705511.2022.2108813

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426.

Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics*, *1*(3), 1–16. https://doi.org/10.1016/j.rmal.2022.100027

Handayani, N. L. P., & Soeparan, P. F. (2022). Peran Sistem Pembayaran Digital Dalam Revitalisasi UMKM. *Jurnal Mahasiswa: Jurnal Ilmiah Penalaran Dan Penelitian Mahasiswa*, *4*(3), 238–250.

Harahap, L. K. (2020). Analisis SEM (Structural Equation Modelling) Dengan SMARTPLS (Partial Least Square). *Fakultas Sains Dan Teknologi Uin Walisongo Semarang*, (1), 1.

Mariani, Suryani, E., Saufi, A., & Soesetio, R. R. A. (2024). Implementation of SEM Partial Least Square in Analyzing the UTAUT Model. *American Journal of Humanities and Social Sciences Research*, *8*(2), 215–224.

Nupus, H. (2025). *Pengaruh Cyber Crime dan Persepsi Keamanan Terhadap Tingkat Kepercayaan Pengguna Produk E-banking (Survei Pada Pengguna E-banking Bank Syariah di Indonesia*. *1*(3), 102–116.

Putu, N., Dewi, A., Made, I., & Wibawa, A. (2023). *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana Pengaruh Perceived Organizational Support Terhadap Kinerja Karyawan Dengan Employee Engagement Sebagai Variabel Mediasi*. *12*(03), 450–459.

Ramadhan, B., Sari, E. P., Julira, J., Meitrisia, M., Amelia, R., Roswita, T., & Sapitri, S. (2025). Pengaruh Diferensiasi Produk, Strategi Harga, dan Saluran Distribusi terhadap Daya Saing Produk Vaseline di Kalangan Mahasiswa di Palangkaraya. *Jumbiwira: Jurnal Manajemen Bisnis Kewirausahaan*, *4*(2), 57–75.

Safaria, T., Rahayu, Y. P. R., & Rahaju, S. (2024). Adaptasi Skala Parent Child Relationship (IPPA) Versi Indonesia. *Jurnal Psikogenesis*, *12*(2), 146–161.

Sari, S. N., & Fitri, A. O. (2025). Analisis Persepsi Masyarakat Terhadap Keamanan Dan Risiko Cyber Crime Dalam Perbankan Digital. *Inflasi: Jurnal Ekonomi, Manajemen Dan Perbankan*, *2*(1), 77–83.

Sholiha, E. U. N., & Salamah, M. (2016). Structural equation modeling-partial least square untuk pemodelan derajat kesehatan kabupaten/kota di Jawa Timur (studi kasus data indeks pembangunan kesehatan masyarakat Jawa Timur 2013). *Jurnal Sains Dan Seni ITS*, *4*(2).

Sholihin, M., & Ratmono, D. (2021). *Analisis SEM-PLS dengan WarpPLS 7.0 untuk hubungan nonlinier dalam penelitian sosial dan bisnis*. Yogyakarta: Penerbit Andi.

Sofyani, H. (2025). Penggunaan Teknik Partial Least Square (PLS) dalam Riset Akuntansi Berbasis Survei. *Reviu Akuntansi Dan Bisnis Indonesia*, *9*(1), 80–94.