PLS-SEM approach in measuring the impact of influencing factors on user's perceived security and trust in e-payment – The case of rural areas in Vietnam

Thi-Duong, Nguyen[1]* and Ke-Duc, Le[2]

[1]. The International School, Duy Tan University, Danang, Vietnam.
[2]. The Electric and Electronic Department, Duy Tan University, Danang, Vietnam.

DOI: 10.29322/IJSRP.11.04.2021.p11249
http://dx.doi.org/10.29322/IJSRP.11.04.2021.p11249

Abstract- Since the Covid-19 has boomed all over the world, most of the transactions were conducted online even in the rural or remote areas in Vietnam. The majority of population stayed at home with devices connected to internet, which increased the e-commerce transaction not only within domestic but also the cross-border transactions. Along with it, the 3G and 4G availability in most of cities and provinces in Vietnam has increased the access to the internet with 54 percent of Vietnam's population accessing the internet. As a result, the e-payment transactions have increased significantly. Although, the increase in e-payment transactions and the attitude of the public towards e-payment has been encouraged over the past few years, Vietnam still is one of the countries that has the highest cash payments in the Association of Southeast Asian Nations region as the results of the issues of customer awareness of security and trust in electronic payment system. The perception of security and trust has still been the barrier that prevents the use of e-payment methods in Vietnam, especially in the rural areas. The current study aims to find out factors affecting the perceived security and perceived trust in e-payment of people who are living in the rural areas in Vietnam.

Index Terms- Perception of Security, Perception of Trust, E-payment, Rural areas in Vietnam.

I. Introduction

Paying for goods and services electronically is not a new idea. The electronic payment (e-payment) system started in early 1997. Nowadays, e-payment has become popular method thanks to its convenience (Özkan et al., 2010).

E-payment systems enable a customer to pay for the goods and services online instead of using traditional payment methods. Its main objectives are to increase efficiency and most of all to enhance customer's convenience. Thank to its convenience and advantages, e-payment is expected to take over the cash in payment method not only in the developed countries but also in developing economic. We have experienced the transformation of payment method in Vietnam market over the last decade. It was found in the part that there was more than 90 percent of payment transaction in Vietnam was conducted in cash and only one-third of Vietnam's population having a bank account (Das, 2017). At that time, access to traditional banking service in remote or rural areas remain low due to the difficulty in accessing to the Internet in those areas. According to Das (2017), security issues was considered as the major factor preventing Vietnamese citizen from using e-payment with over 50 percent of users had expressed concerns about security issues in e-payment.

According to the survey conducted by the Ministry of Industry and Trade of Vietnam, cash and bank transfers were the most popular forms of payment for buyers in the period 2015-2017. E-wallets payment on the other hands significantly 26% over the same period, while payment cards rose 20 percent. Lack of internet penetration, bank account and confidence in e-payment caused the little incentive to move away from cash to online payment (Nguyen et al., 2018) over period 2015-2017. However, the situation changed from 2019 due to the Covid-19. Since the Covid-19 has boomed all over the world, most of the transactions were conducted online even in the rural or remote areas. The majority of population stayed at home with devices connected to Internet, which increased the e-commerce transaction not only within domestic but also the cross-border transactions.

For domestic e-commerce activities, buyer can choose both pay online and pay by cash. On the other hand, only e-payment method is accepted for cross-border transaction. This has made card become the dominant payment method in Vietnamese e-commerce. Bank transfer and digital wallet were ranked second third respectively. Nevertheless, cash still persist with the percentage of transaction conducted by cash about 19%.

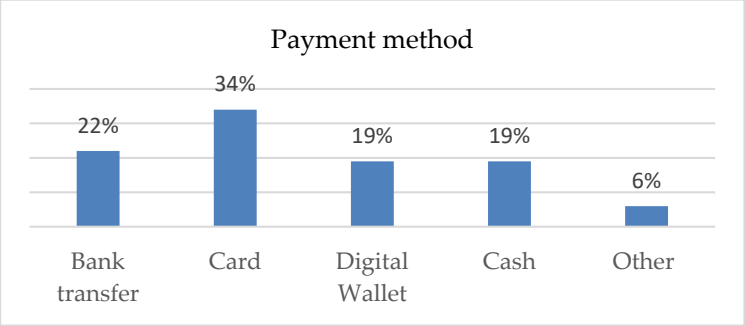

Figure 1.1. Payment methods in Vietnam market (Morgan, 2019)

The question raising is while other country such as China is very successful in eliminate cash transaction and promoting e-payment methods, cash still persist in Vietnam. The answer lies in

the challenges related to network security risk such as fraud, customer fraud, network attacks and the user data leakage along with customer trust and an inadequate legal framework are roadblocks to the transformation of payment method in Vietnam. Since most of Vietnamese users are not very familiar with the technical details of e-payment method, especially, for user's living in remote and rural areas. Therefore, they perceive security and trust based on the basis of their experiences. Thus, besides the adequate legal framework of government, eliminating user's concerns of security problems will help in enhancing user's trust in e-payment transaction, from that can promote the use of e-payment in Vietnam.

This study aims to explore underlying factors that have significant influence on user's perception of security and perception of trust in e-payment system with the following specific objectives:

- To find out factors that have significant influence on Vietnamese user's perceived security and perceived trust in e-payment, the case study in the rural areas in Vietnam.
- To explore how the factors affect user's perceived security and perceived trust in e-payment.

II. Review on previous studies

This section reviews the relevant previous studies in order to identify factors that have effect on user's perception of trust and security in e-payment methods. The factors then will be developed to construct the conceptual foundation and research framework.

As mentioned in the previous section, security and trust are two major issues in e-payment. These issues have often been discussed when referring the electronic payment and many studies have supported that the perceived security and trust significantly influence user's adoption of e-payment []. Additionally, perceived security leads to user's trust (Kim et al., 2010). The lack of safety and trust are the main causes of hesitating to use e-payment. According to the depth study of Hudaib et al. (2014), online payment was safe. However, in reality, the security of e-payment depended much more on the user's perception. Don't know how to use the internet or e-commerce website were sometimes perceived as unsecured by users. Urs et al. (2013) indicated that the security issues of e-payment changed quickly and constantly. Therefore, security was considered as an extremely essential requirement for e-payment. Vinitha et al. (2017) confirmed security was the main concern when the payment was made electronically, in which the fear of privacy information might be stolen was considered as one of the most concerns of e-payment users. According to Huang et al. (2012), privacy was a conflicting issue between consumers and merchants as the users would like to keep their information and details of transaction private while merchant would like to record appropriate and sufficient details of consumers and transaction.

Since e-payment operates without the direct control of human for individual transactions. It might be attacked (Kim et al., 2010). Therefore, e-payment system needs to have the technical infrastructure to ensure the attack will be not happen or in the other word, to assure that the risk of attack will be reduce. User's perceived security is the valuation on the system and how well they are protected against potential risk (Linck et al., 2006). Therefore, technical protection which plays as a safeguard is vital in e-payment system. The elements of technical protections such as integrity, privacy and stability should enhance the perceived security and trust of digitalised transactions (Oney et al., 2017). Findings previous studies [Kim et al., 2010; Oney et al., 2017; Ooi et al., 2020; Yoon and Ocena, 2015; Abdullah and Saleh, 2019) supported the statement that technical protection have significant impact on consumer's perceived of security and trust.

The second factors mentioned much in the context of e-payment is transaction procedures which is designed to facilitate user's adoption of e-payment by bringing the convenience mechanisms (Kime et al., 2010). According to Oney et al. (2017), transaction procedure in e-payment can be divided into three stages. The first stage is authentication, the second stage is the guideline to complete the transaction and the final stage is acknowledgement. These three stages are believed to increase the confidence of users and eliminate user's perception of unsafety. Thus, it can increase the perceived of security and trust. According to Romdhane (2005), if the transaction procedure is well-designed to bring the convenience to users, it will satisfy their security requirement and eliminate their concerns about security and trust.

Security statement in EPS which is defined as the necessary information about how to carry out the e-payment transactions and security solutions supported to consumers, have also been discussed frequently in prior literature. User's trust was confirmed to be perceived by the security statement in e-transactions (Kim et al., 2010). Users tend to be reluctant to use e-payment if they remain unaware of security that is inherent to their transactions (Yoon, 2002). Moreover, the quality of security statement influences user's perception of security and trust. Therefore, in order to enhance the perceived security and trust, security statement should be provided to users in the attractive way to capture their attention. Additionally, security statement needs to be accurate and easy enough for user to understand as user's knowledge of security of e-payment transaction is determined by the understanding of security statement provided to them.

III. Methodology

Although security and trust have a vital role in the user's behaviour of e-payment use, not many imperial studies undertaken to investigate the determinants of perceived security and trust and examine the direct relationship between user's perceived security and perceived trust in e-payment have been found in the literature. The notable exception includes the study of Chellappa and Pavlou (2002); Kim et al. (2010); Oney et al. (2017) and Ooi et al. (2020). This study followed the model proposed by the study of Kim [16]. The model then developed and applied in the case of e-payment system in Vietnam e-commerce market. The study of Kim et al. (2010) examined factors driving user's perceive security and trust toward e-payment. Factors related technical protections, transaction procedures, security statement were considered as e-Payment objective dimension that have significant influence on user's perceive security and perceive trust in e-payment, from that influence the use of e-payment. Findings of the study of Kim found two out of three factors had significant on consumer's perceive security and trust that were technical protections and security statement while the impact of transaction procedure on perceived security was not supported by statistical evidence.

Moreover, the findings also indicated the positive impact of security on trust and e-payment use.

There are 9 hypotheses proposed as below:

H1: Technical protections have a positive and significant impact on user's perceived security in e-payment

H2: Technical protections have a positive and significant impact on user's perceived trust in e-payment

H3: Transaction procedures have a positive and significant impact on user's perceived security in e-payment

H4: Transaction procedures have a positive and significant impact on user's perceived trust in e-payment

H5: Security statements have a positive and significant impact on user's perceived security in e-payment

H6: Security statements have a positive and significant impact on user's perceived trust in e-payment

H7: User's perceived security has positive and significant impact on user's perceived trust in e-payment

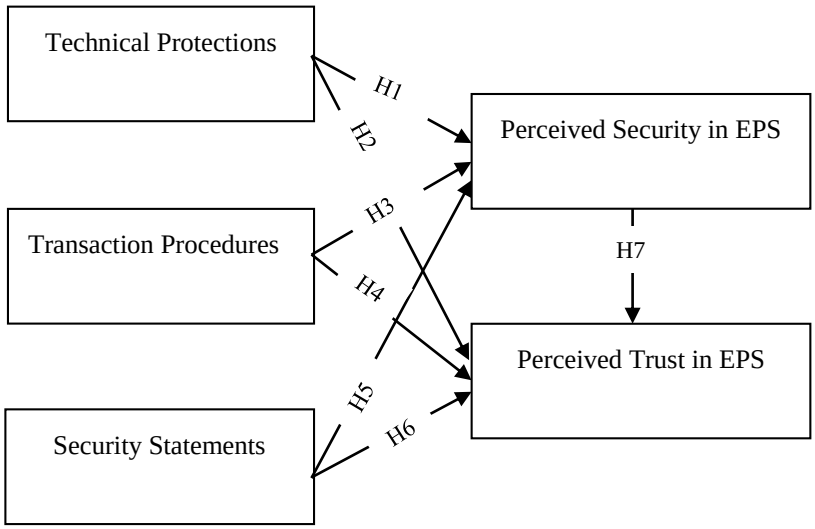

Figure 3.1: Research Model

To achieve the research's objective, primary data were collected from conducting an online survey.

In all cases, the online survey conducted, the respondents complete the questionnaire on their own. By using online survey, the respondents are able to answer the questionnaire without any disturbing of interviewer. Therefore, this appears to be a good way to eliminate bias from interviewer's opinion. As our sample aims to people living in the rural areas who are not familiar with google docs, that why the survey was posted on popular social networks such as Facebook and Zalo. The author tried to reach as many respondents as possible. Therefore, the survey was available online for 3 months. With exclusion of incompleted or missing questionaires, the research was applied to a total of 212 respondents.

The survey was divided into three parts.

The first parts asked 8 questions about respondent's personal information such as name, age, gender, etc. The second part asked respondents 4 questions related to their experience of e-payment with multiple choices. The third part contains 27 questions related to the research's variables. These questions will be scored by using a five-point Likert scale (Brown, 2010). Table 3.1 describes the measurement of the three factors that assumed to have impact on user's perceived security and trust in e-payment.

Table 3.1. Measurement of influencing factors

Influencing factors	Measurement	References
Technical Protections	Privacy; Integrity; Confidentiality	Kim et al. (2010) [16]
Transaction Procedures	Authentication; Modification; Confirmation.	Kim et al. (2010) [16]
Security Statement	Availability; Accessibility; Comprehensibility.	Kim et al. (2010) [16]

For quantitative data analysis, the Partial Least Squares (PLS) is applied as a method for Structural Equation Modelling (SEM) with common evaluation such as coefficients of determinant (R square), validity test, and path coefficient. Concept and results of these will be discussed in next section.

IV. Empirical Results

This section presents the demographic analysis, R-square, bootstrapping, validity testing, hypothesis testing and VIF testing. Before going to further analysis, the model must firstly fit. To measure the model's fit, the value of Standardized Root Mean Square Residual (SRMR) less than or equal 0.08 are considered a

good fit. In this research, the SRMR value equal to 0.074, indicating good fit model.

1.1. Descriptive Statistics

The demographic analysis of total 212 respondents are summarized in Table 4.1.

Table 4.1. Respondents' General Information

	Category	Frequency	Percentage
Gender	Male	93	43.9%
	Female	119	56.1%
Age	<20	69	32.5%
	20-35	94	44.3%
	36-50	40	18.9%
	51-65	7	3.3%
	>65	2	0.9%
Marital Status	Single	114	53.8%
	Married	98	46.2%
Areas	North	78	36.8%
	Middle	43	20.3%
	South	91	42.9%
Career	Worker	37	17.5%
	Office Staff	16	7.5%
	High school- student	25	11.8%
	Farmer	62	29.2%
	Retired	4	1.9%
	Teacher	43	20.3%
	Other	25	11.8%
Monthly Income	< US$300	151	71.2%
	US$300-US$500	49	23.1%
	>US$500	12	5.7%
Total		**212**	**100.00%**

It is noted that most of the respondents are female (56.1%). Which is not surprising as in rural areas in Vietnam, women are supposed to be the one who is in charge of shopping. Additionally, 32.5% of participants in this survey are younger than 20 and 44.3% is at the age of 20 to 35. Although internet and smart phone are not new, it is not so popular for the old generation in the rural areas in Vietnam. For most people living in rural areas who are older than 50, it is so hard to learn how to connect to the internet and use the smart that they choose to use the phone that has basic functions such as making a phone call and sending messages. Lack of knowledge about technology is the barrier to preventing old people from using smart phone, shopping online and making e-payment. That why the rate of those in this survey is low. Regarding the geography, most of the respondents come from the south and the north of Vietnam with the percentage of 42.9% and 36.8% respectively. 62 of total 212 are farmer accounted for 29.2%, 43 of those are teachers (20.3%), 17.5% is worker and 11.8% is student at high school. Moreover, it is no doubt that the personal monthly income of people living in the rural areas is not very high. Particularly, 71.2% of respondent has the monthly income lower than US$300, 23.1% can earn from US$300 to US$500 per month and 5.7% has the monthly income higher than US$500.

1.2. Validity test

In this stage, the validity is tested. There are two commonly validity assessment in PLS-data based analysis: (1) convergent validity and (2) discriminant validity. Convergent validity measures whether the item of one variable is highly correlated. This is represented by the factor loading which depends on the sample size of data set. In general, the smaller the sample size, the higher the required loading factor. Discriminant validity measures the extent particular constructs in the same model differ from each other (Hair et al., 2017).

In PLS, convergent validity consists three tests: item reliability (Loadings), composite reliability (CR) and average variance extracted (AVE) (Hair et al., 2017).

Item reliability evaluates the loadings of the items with their respective construct (Hair et al., 2017). Some previous researches argued that a value of 0.5 might be acceptable as long as the other items in the same contract have higher loadings value (Hair et al., 2017). However, the conservative acceptable value of item reliability is 0.7.

Composite reliability is a measure of scale reliability, which is used assesses the internal consistency of particular construct. The threshold of composite reliability is 0.7.

AVE presents the average amount of variance in indicator variables that a construct is managed to explain. AVE must be greater than 0.5 to be acceptable (Hair et al., 2017).

The results of validity test of five variables are presented in Table 4.2.

Table 4.2. Results of Validity Test

Constructs	Measurement	Loadings	Cronbach's Alpha	CR	AVE
Technical protections	TechP1	0.807	0.862	0.907	0.710
	TechP2	0.810			
	TechP3	0.793			
	TechP4	0.771			
	TechP5	0.709			
	TechP6	0.731			
	TechP7	0.745			
Transaction Procedures	Trans1	0.874	0.857	0.893	0.582
	Trans2	0.878			
	Trans3	0.882			
	Trans4	0.919			
	Trans5	0.789			
Security statement	SeSt1	0.746	0.883	0.909	0.589
	SeSt2	0.803			
	SeSt3	0.729			
	SeSt4	0.793			
	SeSt5	0.747			
	SeSt6	0.756			
Perceived Security	Secu1	0.805	0.921	0.939	0.756
	Secu2	0.835			
	Secu3	0.788			
	Secu4	0.934			
Perceived Trust	Trust1	0.844	0.875	0.914	0.727
	Trust2	0.848			
	Trust3	0.881			
	Trust4	0.836			

Data in Table 4.2 showed the loadings are all greater than 0.7, the Cronbach's alpha and composite reliability of five variables are all greater than 0.7 and the AVE are higher than 0.5 confirm the validity and reliability of all constructs.

Discriminant validity is tested by using square roots of AVE and/or cross loadings test (Hair et al., 2017). Table 4.3 reported Fornell-Larcker Criterion while Table 4.4 showed the results of cross-loadings.

Table 4.3. Fornell-Larcker Criterion.

	Perceived Security	Security Statement	Technical Protections	Transaction Procedures	Perceived Trust
Perceived Security	**0.843**				
Security Statement	0.780	**0.763**			
Technical Protections	0.708	0.516	**0.767**		
Transaction Procedures	0.214	0.136	0.169	**0.870**	
Perceived Trust	0.737	0.644	0.650	0.328	**0.852**

According to data in Table 4.3 square roots of AVE of all constructs are higher than squared correlations for each construct. For example, the square roots of AVE of Perceived security has the value of 0.843 which is higher than squared correlations for Security statement (0.780), Technical protections (0.708), transaction procedures (0.214) and Perceived trust (0.737). Data in Table 4.4 presented loadings of the items in its construct (in bold marking) are higher than its loadings on other constructs. Results of square roots of AVE and cross-loadings confirm the adequate discriminant validity.

Table 4.4. Cross-Loadings

Items	Perceived Security	Security Statement	Technical Protections	Transaction Procedure	Perceived Trust
SeSt1	0.485	**0.746**	0.346	0.058	0.428
SeSt2	0.544	**0.803**	0.361	-0.014	0.473
SeSt3	0.492	**0.729**	0.319	0.071	0.467
SeSt4	0.648	**0.793**	0.404	0.192	0.533
SeSt5	0.696	**0.747**	0.476	0.155	0.530
SeSt6	0.647	**0.756**	0.426	0.124	0.493
Secu1	**0.805**	0.643	0.593	0.222	0.588
Secu2	**0.835**	0.624	0.575	0.187	0.609
Secu3	**0.788**	0.672	0.536	0.045	0.593
Secu4	**0.934**	0.689	0.675	0.258	0.688
TechP1	0.560	0.449	**0.807**	0.116	0.525
TechP2	0.554	0.431	**0.810**	0.136	0.557
TechP3	0.580	0.505	**0.793**	0.097	0.507
TechP4	0.650	0.468	**0.771**	0.134	0.574
TechP5	0.492	0.286	**0.709**	0.147	0.427
TechP6	0.471	0.299	**0.731**	0.124	0.414
TechP7	0.458	0.278	**0.745**	0.161	0.453
Trans1	0.085	0.093	0.054	**0.874**	0.234
Trans2	0.149	0.099	0.127	**0.878**	0.271
Trans3	0.111	0.069	0.110	**0.882**	0.245
Trans4	0.200	0.075	0.145	**0.919**	0.281
Trans5	0.295	0.203	0.229	**0.789**	0.340
Trust1	0.560	0.524	0.476	0.314	**0.844**
Trust2	0.644	0.562	0.549	0.200	**0.848**

Trust3	0.689	0.615	0.610	0.311	**0.881**
Trust4	0.610	0.486	0.572	0.292	**0.836**

1.3. Structure model

The structural model evaluation relates to the measurement collinearity, coefficients of determination. Collinearity refers to the high correlation between two constructs. However, if there are the high correlation between more than two constructs, there will be the multicollinearity problem, which means one or more constructs in the research model are redundant. To make sure there is no multicollinearity, the Variance Inflation Factor (VIF) value is used with a threshold of 5 (Franke, 2010).

Table 4.5 indicated the VIF value of all construct are lower than 5, which mean that there is no multicollinearity problem. Therefore, no variable in this research is eliminated.

Table 4.5. Collinearity Statistics (VIF)

Constructs	Perceived Security	Perceived Trust
Perceived Trust		
Perceived Security		3.841
Security Statement	1.368	2.571
Technical Protections	1.382	2.019
Transaction Procedures	1.033	1.051

Coefficients of determination (R^2) are presented in Figure 4.1 which indicated high R^2 for both perceived security (0.740) and perceived trust (0.623). The good VIF value and high value of coefficients of determination support the good model structure.

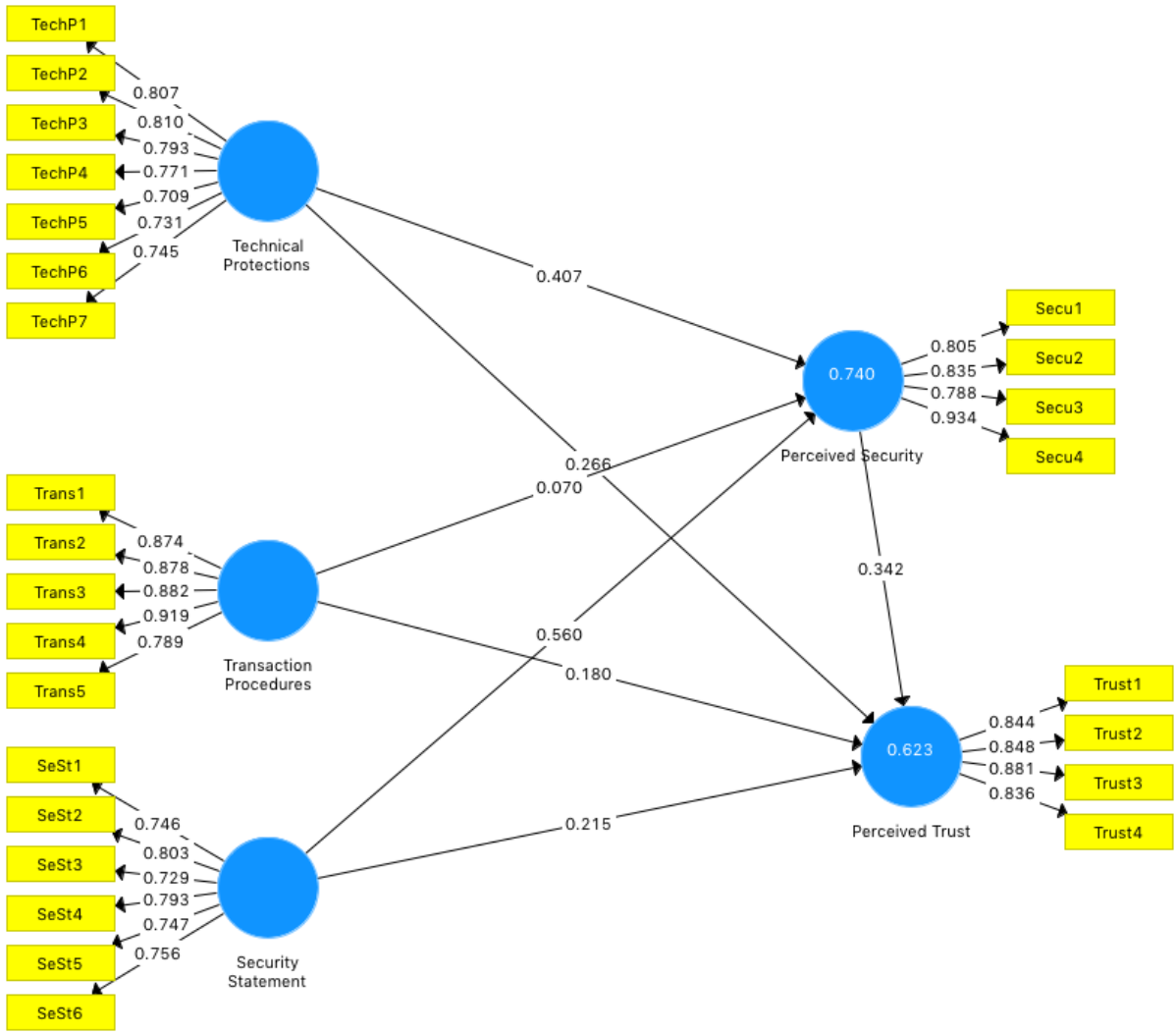

Figure 3.1. Factors affecting user's perceived security and perceived trust in e-paymentbased on a PLS-SEM model.

1.4. hypotheses Testing

After being confident that there is no multicollinearity between constructs in this study, the results of hypothesis testing are showed at table 4.5 below.

Table 4.5. Results of Hypothesis Testing

Hypothesis	Path Coefficient	T Value	P Values	Results
Perceived Security -> Perceived Trust	0.342	3.362	0.000	Supported
Security Statement -> Perceived Security	0.560	11.769	0.000	Supported
Security Statement -> Perceived Trust	0.215	2.832	0.004	Supported
Technical Protections -> Perceived Security	0.407	8.919	0.000	Supported
Technical Protections -> Perceived Trust	0.266	3.825	0.000	Supported
Transaction Procedures -> Perceived Security	0.070	2.215	0.044	Supported
Transaction Procedures -> Perceived Trust	0.180	2.826	0.002	Supported

[1]

Since the path coefficients of all constructs are significant at $p < 0.05$, all research hypotheses are supported. However, the impact level of each influencing factor on user's perceived security and perceived trust are different.

Security statements has the highest impact on user's perceived security in e-payment, proved by the path coefficient of 0.560 with T-value if 11.229 and p-value lower than 0.05. However, the effect of security statements on perceived trust is much lower at 0.215 with t-value of 2.832 and p-value lower than 0.05. Therefore, it can be concluded that despite positive influence in perception of security and trust, security statements tend to affect more on user's perceived security.

Technical protections such as privacy; integrity; confidentiality have a positive and significant effect on both user's perceived security and perceived trust with path coefficient of 0.407 and 0.266 respectively. Like security statements, technical protections seem to have more impact on perceived security than on perceived trust.

Transaction procedures found to have positive on both perceived security and perceived trust. However, the effect on user's perceived security is low at 0.07 with small t-value of 2.215 and p-value of 0.044 while the effects on perceived trust is higher at 0.180 with t-value of 2.826.

Perceived security fond to have positive and significant influence in perceived trust with the path coefficient of 0.342 with t-value of 3.362.

V. Conclusion and Discussions

The main objective of this research is to find out factors influencing user's perceived security and perceived trust in e-payment applied in the case of people living in the rural areas in Vietnam. The author followed the research model of Kim et al. (2010) which assumed three factors having positive and significant impact on consumer's perception of security and trust: (1) technical protections, (2) transaction procedures and (3) security statements. This research has both common findings with the results of Kim et al. (2010) and different findings.

Firstly, both the findings of Kim et al. (2010) and this research's findings supported that technical protections and security statements have positive and significant impact on use's perceived security and perceived trust in e-payment. Additionally, transaction found to have influence on perceived trust.

Technical protections play an important role in user's perceived security and trust. If users aware that their personal information are protected by not being released to other parties when making e-payment transaction and the amount of payment transaction are accurate, they will perceive e-payment is safe. To do that, stable maintaining for integrity and confidentiality is necessary.

Security statements are the necessary information about how to carry out the e-payment transactions and security solutions supported to users. Therefore, reducing the security concerns of users by focusing more on commitments, the quality of details in designing security statements and posting them directly on their sites are the good solution to enhance perceived security and trust. The different finings is that while Kim et al. (2010) found that no statistical evidence to support that transaction procedures have significant influence in perceived security of user, this research found the positive relationship between these two variables supported by p-value of 0.044. However, the influence of transaction procedures on perceived security is low at 0.07 (path coefficient). One of the most prominent reasons explains why users in rural areas in Vietnam do not tend to use e-payment instead of cash is that the e-payment methods provide the sophisticated transaction procedures, which make users have difficulty in understand and follow to complete the payment transaction. It is understandable that e-payment provider would like to enhance the security of the system; however, from the user's perspective; they perceived these procedures as sophisticated, not ease to use and inconvenience.

References

[1] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[2] Abdullah, R., & Saleh, Y. (2019). Factors affecting buyers' trust in e-commerce in Palestine. Middle East Journal of Management, 6(5), 597-639

[3] Barkhordari, M., Nourollah, Z., Mashayekhi, H., Mashayekhi, Y., & Ahangar, M. S. (2017). Factors influencing adoption of e-payment systems: an empirical study on Iranian customers. Information systems and e-business management, 15(1), 89-116

[4] Brown, S. (2010). Likert scale examples for surveys. ANR Program evaluation, Iowa State University, USA.

[5] Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management

[6] Chen, A., Zeltmann, S., Griffin, K., Ota, M., & Ozeki, R. (2020). Demographic background, perceptions, and e-payment usage among young Japanese. Glob J Bus Discip, 4(1), 4

[7] Das, K. (2017, July 12). Vietnam's Payment Preferences: four Trends to Watch. https://www.vietnam-briefing.com/news/vietnams-payment-preferences-4-trends-watch.html/

[8] Franke, G. R. (2010). Multicollinearity. Wiley international encyclopedia of marketing.

[9] Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. International Journal of Multivariate Data Analysis, 1(2), 107-123.

[10] Huang, E., & Cheng, F. C. (2012). Online security cues and e-payment continuance intention. International Journal of E-Entrepreneurship and Innovation (IJEEI), 3(1), 42-58.

[11] Hudaib, A. A. Z. (2014). E-payment security analysis in depth. International Journal of Computer Science and Security (IJCSS), 8(2014), 14.

[12] Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. Electronic commerce research and applications, 9(1), 84-95.

[13] Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). Security issues in mobile payment from the customer viewpoint

[14] Morgan, J.P. (2019). E-commerce Payments Trends: Vietnam. https://www.jpmorgan.com/merchant-services/insights/reports/vietnam

[15] Nadler, S., Chen, A. N., & Lin, S. F. (2019). E-payment usage among young urban Chinese. The Journal of Business Diversity, 19(3), 75-88

[16] Nguyen, C., Dinh, D., & Doan, T. (2018). The Determinants of the Choices of Payment Methods for Goods and Services Transaction in Vietnam. International Journal of Applied Science, 1(2), p84-p84.

[17] Oney, E., Guven, G. O., & Rizvi, W. H. (2017). The determinants of electronic payment systems usage from consumers' perspective. Economic research-Ekonomska istraživanja, 30(1), 394-415

[18] Ooi, S. K., Ooi, C. A., Yeap, J. A., & Goh, T. H. (2020). Embracing Bitcoin: users' perceived security and trust. Quality & Quantity, 1-19

[19] Özkan, S., Bindusara, G., & Hackney, R. (2010). Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis. Journal of enterprise information management.

[20] Putri, Y. E., Wiryono, S. K., Nainggolan, Y. A., & Cahyono, T. D. (2019). Method of payment adoption in Indonesia e-commerce. The Asian Journal of Technology Management, 12(2), 94-102

[21] Romdhane, C. (2005). Security implications of electronic commerce: A survey of consumers and businesses. Internet Research: Electronic Network Applications and Policy, 9, 372–382.

[22] Salloum, S. A., Al-Emran, M., Khalaf, R., Habes, M., & Shaalan, K. (2019). An Innovative Study of E-Payment Systems Adoption in Higher Education: Theoretical Constructs and Empirical Analysis. International Journal of Interactive Mobile Technologies, 13(6)

[23] Urs, B. A. (2015). Security issues and solutions in e-payment systems. Fiat Iustitia, (1), 172-179

[24] Vinitha, K., & Vasantha, S. (2017). Factors Influencing Consumer's Intention to Adopt Digital Payment-Conceptual Model. Indian Journal of Public Health Research & Development, 8(3)

[25] Xena, P., & Rahadi, R. A. (2019). Adoption of e-payment to support small medium enterprise payment system: A conceptualised model. International Journal of Accounting, 4(18), 32-41.

[26] Yoon, H. S., & Occena, L. G. (2015). Influencing factors of trust in consumer-to-consumer electronic commerce with gender and age. International journal of information management, 35(3), 352-363.

[27] Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. Journal of interactive marketing, 16(2), 47-63

AUTHORS

First Author – Thi-Duong, Nguyen, The International School, Duy Tan University, Danang, Vietnam. Email: nguyenthiduong1@dtu.edu.vn
Second Author – Ke-Duc, Le, The Electric and Electronic Department, Duy Tan University, Danang, Vietnam. Email: lekeduc@dtu.edu.vn

Corresponding author's email: nguyenthiduong1@dtu.edu.vn