ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse97842019.pdf
https://doi.org/10.30534/ijatcse/2019/97842019

Assessing the Security Factors in QR-based Mobile Payment in Indonesia

Azelika Rulyfayrizqi[1], Risma Nurdyani[2], Suryatining Wahyu Pamenang[3], Gunawan Wang[4]
[1]Information Systems Management Department, BGP-Master of Information Systems Management
Bina Nusantara University, Jakarta, Indonesia. e-mail: azelika.rulyfayrizqi@binus.ac.id
[2]Information Systems Management Department, BGP-Master of Information Systems Management
Bina Nusantara University, Jakarta, Indonesia, e-mail: risma.nurdyani@binus.ac.id
[3]Information Systems Management Department, BGP-Master of Information Systems Management
Bina Nusantara University, Jakarta, Indonesia, e-mail: suryatining.pamenang@binus.ac.id
[4]Information Systems Management Department, BGP-Master of Information Systems Management
Bina Nusantara University, Jakarta, Indonesia, e-mail: gwang@binus.edu

ABSTRACT

Mobile payment (M-Payment) has emerged dynamically from year to year. With the increasing use of mobile technology by consumers, their lifestyle choices continue to evolve as well as a few different economic factors. This research proposes an expanded UTAUT Acceptance research model to see the actual use of QR-based mobile payment users. The proposed research model was tested and validated using data collected by a survey of 129 Indonesian citizens. This research used security-related factors such as social influence, facilitating condition, security, trust, and privacy risk to evaluate its impact to the customer intention of use QR-based mobile payment. A total of 123 respondents participated in this research. The findings revealed that privacy risk and security were positively related to the customer intention of use QR-based mobile payment. This research provided the practical and theoretical implications of these findings.

Key words : Mobile Technology, QR-based Mobile Payment, Security, UTAUT.

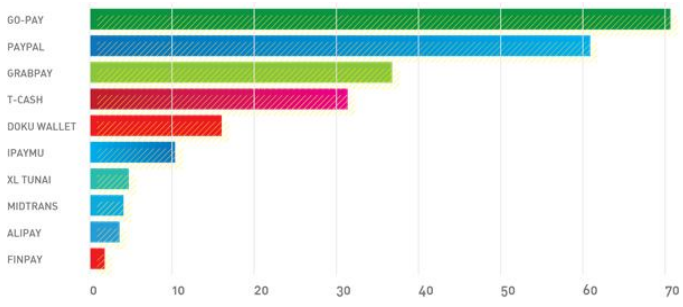
1. INTRODUCTION

Mobile modes of payment are becoming popular in the last few years, American political economy Robert Reich predicts for sure that the time will come when the era of cash or cash payments will end, even if he is not sure when it will arrive. His belief is related to the lifestyle of the American people who are now doing more non-cash transactions, even for “coins” transactions, such as parking fees, toll fees, and buying cakes on the roadside. Cellular payments have been adopted by all over the world in various ways. All types of cellular payments on the combined market are expected to reach more than $ 600 billion globally in 2013. Benchmarking to the Chinese market, for now there are only 2 biggest cellular payment players, Alipay; WeChat Pay. They currently control almost 90% of the cellular payment market share in China [1].

The benefits currently offered by m-payments are compared to traditional payment methods including aspects of comfort, cost, security, and other benefits, such as the ability to receive advertisements and check balances everywhere.

Over the past few years, the term "Community without Money" has been promoted by Bank Indonesia (BI). Bank Indonesia is the central bank of Indonesia which pioneered the "National No Money Movement" in 2014, the aim of which is to provide convenience for each user and reduce the cost of handling financial institutions. David Wolman in his book "The End of Money" explains that cash transactions are currently very expensive, and they have played an "enemy" for the bank itself, because banks still need cash manually, and in this way can increase operational costs bank. On a macro scale, transactions conducted on a non-cash basis can be more transparent and accountable [2].

It can be seen from the following figure that of the 10 most popular mobile payment in Indonesia, almost all are supported by large investors or companies with a lot of money to burn (For example, Go-Pay on Go-Jek's is supported by KKR & Warburg Pincus; Grabpay on Grab's is supported by Softbank, T-Cash Telkomsel is owned by Telkom Indonesia,



(figure 1.).

Figure 1: Popular Mobile Payments in Indonesia [3]

Many Mobile payment services in Indonesia subsidize every transaction through cashback, discounts through collaboration with several traders to increase the use of cellular payments. The opening of space for the purpose of developments in mobile telephone technology in Indonesia opens opportunities for payment-m and helps accelerate financial inclusion programs in Indonesia. Therefore, for the development of m-payments, it is necessary to do mapping, both the m-payment implementation mapping itself and the risk mapping contained therein.

Recently, several providers of payment systems based on the QR code system - both banks, technology companies, and digital - have actively attracted users. Efforts to add transactions and the number of QR code users were also carried out by PT Dompet Anak Bangsa. Where companies under the auspices of Go-Jek Indonesia often hold an event titled Go-Food Festival, which presents many culinary traders. In the festival, payment transactions use Go-Pay financial services. So, through his cellphone, Go-Pay users can pay for groceries by scanning the QR code at each of the food outlets. This payment technology has also been used in transportation modes. Residents in Semarang City can use TCash's QR code for Trans Semarang services.

Onny Wijanarko as Head of the Payment System Policy Department of Bank Indonesia (BI), sees that a large number of people who use smartphones will change the payment system landscape in the country. The number of smartphone users rose from 65.2 million in 2016 to 74.9 million last year. On the other hand, BI wants to ensure that payment technology is safe and does not endanger the public. This sees a phenomenon in China that has used many QR codes for non-cash payment transactions. In that country, most transactions use QR codes created by WeChat Pay and AliPay (figure 2). Two payment applications also have 963 million and 520 million active users every month in 2016.

Nama Aplikasi	Jumlah Pengguna	Jumlah Mitra
TCash	25 juta	52 ribu
Go-Pay	20-25 juta	4 ribu
OVO	5-10 juta	300 ribu
Yap!	310 ribu	15 ribu
Doku	2 juta	35 ribu

Figure 2: Popular Mobile Payments in Indonesia [4]

iResearch Consulting Group research shows that funds transacted through QR codes in China rose from U $ 5 trillion in 2016 to US $ 5.5 trillion last year. The Verge reports, there are people who change the QR code belonging to partners with fake ones in China. This practice occurs because QR codes are static or can be attached anywhere. The fake QR code will steal user data such as a personal identification number (PIN). As a result, hackers can steal money belonging to users in the application [4].

2. LITERATURE REVIEW

2.1 Mobile Payment

All transactions such as payment activation, payment confirmation etc, that use phones or other mobile communication devices are classified into the mobile payment system [5]. Nowadays, mobile payment become alternative for almost all payment transactions like online shopping or pay the bills. This payment method can be used by utilizing the wireless communication network technology or other technology communications [6]. Claessens et al., [5] that at present, mobile phones will be developed into personal trust devices. To make the secure payment transactions, wireless transport layer security (WTLS), wireless public key infrastructure (PKI), and other security features are being integrated into mobile technology. While Donner and Tellez [7] suggested that mobile payment and mobile banking are collectively referring to an application that allows people to access mobile banking, transfer funds, and make payments to stores using their mobile phones.

2.2 Security in Mobile Payment

Westin [8] states that customers are very concerns about security and privacy of their transactions. Although Bank Indonesia (BI) has just launched a financial technology office in 2016 which is tasked with evaluating the risk assessment and mitigation of technology companies, especially payment systems operating in Indonesia, but people must be scrupulous while using their electronic, mobile, or switching payment such as debit or credit cards at merchants with no good reputation [9]. Positive perceptions of security should be improved especially in e-commerce [10]. Schierz, Schilke, & Wirtz said on their research that security is one of the factors that significantly influences on person’s trust in the use of mobile payment [11].

2.3 QR Code in Mobile Payment

Peter et al., [12] states that QR codes is a new method of mobile payment that can even be done only by carrying a mobile phone. After people scan the QR-codes, the system will immediately display their website pages of payment services. In Indonesia it can be seen when people scan QR-codes after buying cinema tickets online, then the tickets will automatically be printed out, this is only as far as

"one-click". From research conducted by Bharambe et al,. proving that payment solutions using QR-codes in Android not only give the advantages for customers, but also for merchants [13]. As one of the biggest companies in the payment sector, Paypal has implemented this payment method in many countries. In a study conducted by Goyal et al. 'Mobile handset operability' is a crucial factor. The device used by the user has many variations, therefore one solution to this issue is the implementation of Mobile Payment using QR-Code [37].

2.4 Intention to Use

Intention of use is the behavior or attitude of users that tends to continue using a technology [14]. Fishbein and Ajzen [15] said that intention to use of technology is closely related to one's tendencies and their behavior. People who like to invest in stocks will often use stock applications, people who like to shop online will often use e-commerce aplications. This also relates to a person's needs. The level of user of a computer technology individually can also be seen by the desire to use an application on an ongoing basis or the desire to motivate others to use that application [16].

2.5 Social Influence

Social influence shows that an individual has the desire to use an application after hearing the experience or recommendations of others [17]. Venkatesh et al., [18] addressed that social influence can be defined as the level at which a person feels that someone else is convincing himself that he must use a new system. While Moore & Benbasat [19] in Chang (2012) state that by using new technology, a person can be considered as having a popular status among their environment. Even someone's behavior can be influenced by beliefs in how others see them as a result of using technology.

2.6 Facilitating Condition

Yifan Chen and Wolfram Salmanian [20] state that when someone's belief to accept a technology is influenced by the facilities, the source provided, or the network, then it is included in the facilitating condition factor. Facilitating conditions is the level of one's belief that the company's infrastructure and technology are available to increase support for system usage [21]. Provided by the organization and technical devices that support the use of a system, facilitating conditions are able to describe the level of an individual in receiving a technology based on the support of facilities. The device can be in the form of a system used, training, manual or other books [17]. Research conducted by Micheni et al. also stated that Faciilitating Condition is a crucial factor in its application in a developing country [38].

2.7 Trust

Rotter [22] said that if someone has expectations of words or promises from other people can be accounted for then that is called trust. Many experts have defined trust. In the context of e-commerce, [23] (in Rusdin, 2007) define trust as a firm's belief in other companies that other companies will provide positive outcomes for the company. Whereas Mayer [24] provides a definition of trust in another definition expressed as the desire of a party to surrender or accept actions from others hope that the other party will do something important for the party who gives trust.

2.8 Security

According to Desmayanti [25] information system security is the existence of management that can prevent, overcome and protect information systems from actions that can harm such as unauthorized use, infiltration of various information needed. The customer's perceived security when carrying out online transactions depends on how one understands the level of security measures taken by the seller [26]. Research result by Oliveira et al., [11] shows that construct variable such as social influence, innovativeness, perceived technology, performance expectancy, compatibility, and also security significantly impacting on the use of mobile payment technology.

2.9 Privacy Risk

Kim, Ferrim, and Rao [27] state that perceived privacy is the perception that someone feels confident that their important and personal information has been safely protected by the company. According to Hanafi [28], Risk is a danger, a consequence or consequence that can occur due to an ongoing process or future event. Risk can be interpreted as a state of uncertainty, where if an unwanted situation occurs it can cause a loss. So it can be taken that privacy risk is a risk that is a concern about the consequences of losing or disclosing personal information to a second party. For example, the company can record name, phone number, e-mail, home address or other client's personal information during a transaction in online trading [29].

3. RESEARCH METHOD

3.1 Research Framework

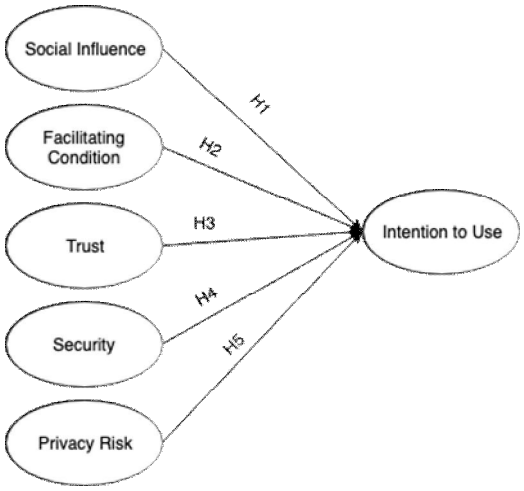


Figure 3 : Proposed Research Framework.

Figure 3 shows the research framework for this article and illustrates five variables namely social influence, facilitating condition, privacy risk, trust, and security. There are five hypotheses in this framework to test the influence of each independent variable on intention of use. The developed framework were adopted from UTAUT model which are Social Influence, Facilitating Condition, and Trust. Several additional variables which are Trust, Security and Privacy Risk were also added in this research framework.

3.2 Data Gathering Method

The primary data for this research are derived from online questionnaire. The questionnaire developed had two parts. The demographic profile, such as Participants' Age, Education Level, and their experience regards the usage of QR-based Mobile Payment on the first part of the questionnaire. The second part of the questionnaire solicits responses on the key constructs of the research framework namely, social influence, facilitating condition, trust, security, and privacy risk. SmartPLS software was used to analyse the data with regression analysis.

The questionnaire used a Likert scale of 5 with 1 being "strongly disagree" to 5 "strongly agree". Online Questionnaires were distributed on May, 2019 to 300 respondents around Kemanggisan, West Jakarta and delivered through Whatsapp and LINE group chats.

Table 1 : The List of Items and Sources

Variables	Indicators		References
Social Influence (SI)	influence behavior to use QR-based Mobile payment.	SI1	[21]
	QR-based Mobile payment	SI2	
	important use of QR-based Mobile payment	SI3	
Facilitating Condition (FC)	necessary resource to use QR-based Mobile Payment.	FC1	[21]
	knowledge necessary to use QR-based Mobile payment.	FC2	
	QR-based mobile payment compatibility.		
	I can get help from others when I have difficulties using QR-based Mobile payment.	FC4	
Privacy Risk (PR)	Losing control over personal information privacy is high..	PR1	[30]
	Loss of privacy without my knowledge.	PR2	
	Keep sensitive information from exposure	PR3	

Trust (TR)	QR-based mobile keep promise.	TR1	[31]
	Keep customer's interest in mind.	TR2	
	Payment service is trustworthy.	TR3	
	Secure transaction for users.	TR4	
Security (SC)	Secure payment systems.	SC1	[32]
	Secure sensitive information.	SC2	
	Safe with sensitive information delivery.	SC3	
Intention to Use (IU)	Predict payment.	IU1	[33]
	Intend to use payment.	IU2	
	Chance to use mobile payment.	IU3	

4. RESEARCH RESULTS

4.1 Profile of Respondents

A total of 129 respondents were participated in this research, and 6 of this were invalid they had never used QR-based mobile payment before, which results to 123 usable responses. It is shown that a majority of the respondents are from the age group of 21-25 years (57.7 %). In terms of education level, most of respondents have bachelor degree (58,5 %).

4.2 Validity and Reliability Test

Validity test is done to measure the questions contained in the questionnaire. Validity is an empirical measurement that describes the true meaning of the concept with consideration. Validity Test measures the accuracy between data that used in this study as an object and the data reported [34]. In this research, validity test was done by using the results of the Loading Factor and AVE (Average Variance Extracted). If the value of AVE less than 0.5 then the indicator is invalid, whereas if the value is greater than 0.5, then it is valid.

Based on the results of the loading factor, there are three invalid indicators because the loading factor value are smaller than 0.7. For this reason, three indicators FC1 (0,495), SC1 (0,524), and SC2 (0,630) must be removed so that the valid path model in this research is as follows:

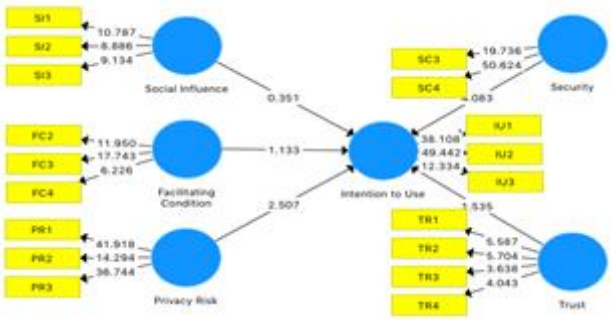


Figure 4 : Path Model.

Same with Validity Test, Reliability Test (Table 2) is done by connecting each indicator with each variable. In this study, the reliability test was done using Composite Reliability and Cronbach's Alpha. If the value of Cronbach's Alpha has a greater value than 0.7 and Composite Reliability also has a greater value than 0.7, then the indicator is reliable, whereas the indicator will not be considered as reliable if the value of Cronbach's Alpha is smaller than 0.7, as well as the value of Composite Reliability.

Table 2 : Reliability Test

Construct	Cronbach's Alpha	Composite Reliability	AVE
FC	0.760	0.856	0.666
IU	0.892	0.952	0.820
PR	0.870	0.919	0.792
SC	0.768	0.893	0.806
SI	0.914	0.946	0.854
TR	0.792	0.858	0.602

Based on the results of the Reliability Test above, it is known that each construct (Facilitating Condition (FC), Intention of Use (IU), Privacy Risk (PR), Security (SC), Social Influence

(SI) and Trust (TR) are reliable because it has a value greater than 0.7.

4.3 The Result of Hypothesis Test

This research used SEM-PLS analysis to test H1 through H5. Bootstrapping of 500 samples and 0.050 (5%) for significant level are used to perform analysis with smartPLS 3.0. In this research, the hypothesis test is done by comparing P-Value with a value of the significant level . If P-Value has a smaller value than the significant level, then the hypothesis is accepted, whereas if the P-Value has a greater value than the significant level, then the hypothesis is not accepted.

Table 3 : Hypothesis Test

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
FC → IU	0.124	0.131	0.114	1.089	0.277
PR → IU	0.315	0.295	0.142	2.225	0.027
SC→ IU	0.442	0.445	0.126	3.520	0.000
SI → IU	-0.108	-0.115	0.110	0.985	0.325
TR → IU	-0.104	-0.066	0.142	0.730	0.466

5. CONCLUSION

The results of this study indicate several consequences that affect researchers and companies. This study also aims to increase the explanatory and predictive power using the UTAUT model in the context of Cellular Payment. Then the researchers investigated some differences in determining the acceptance of the QR-Code to make this payment. Looking at the vital role of security in the context of the new digital environment, namely mobile payments, is a major contribution made by this research. Privacy findings (PR) and security risks (SC) show significant effects on the use of QR-based cellular payments. Where it turns out, security can have a strong direct and indirect effect on the main construction of the model. Proven positively that the existence of security can affect the user's intention to use QR-based cellular payments directly or indirectly. After that, the current investigation is that the authors contribute to the literature review in the UTAUT study by showing the impact of social influence on the intention to use QR-Code-based Mobile Payments. This is an important finding that shows that even though Cellular Payments are not socially accepted, users can still feel comfortable using Cellular payments.

Social influence begins with a widely shared sense of trust in how individual group members must behave in certain situations. Given human behavior that can be influenced by other people's perceptions of how other members of our social groups think and act is a theory that applies in the context of Cellular Payments. Social influence is a non-significant predictor of behavioral intention. In the context of social influence, Cellular Payments do not trigger behavioral intentions. At present, if cellular payments are available, people are more likely to use Cellular Payments for payments anytime and anywhere because it is more practical.

In this study also found empirical findings which indicate that the risks that can arise are multi-dimensional construction for Cellular Payment systems. In this study, the author takes one dimension of risk, namely privacy risk. Privacy risk is related to user concerns about the distribution of user information that is not desirable or can also be called misuse of information. With this connection, it can cause the possibility of missing control of the user's personal information, as well as when information about the user can be used freely without the knowledge or permission of the user himself for things that can harm the user. The emergence of fear and inconvenience to users about the existence of users' personal information published to third parties can have a negative impact on cellular payments. With the existence of this privacy risk, it can further clarify Cellular Payments because smartphones that users have included Internet capabilities and geolocation.

This capability can allow other parties to track what activities the user is carrying out, the location the user visits, and the purchase history of the user. By knowing the existence of these risks, what can be done to prevent this is by requiring special concentration to increase user privacy issues. The conclusion is that users can react negatively to violations of privacy used by other parties. The findings of the research conducted by the authors are that this risk has a negative impact on security.

6. LIMITATIONS

This study has its own limitations which can open the way for future research. the first thing you can do is collect data through an online platform. Where in this study used a sample of 123 respondents. With this limitation, it is expected to prevent generalization of results in the context of the country. then the second thing is data imbalance [35]. Replicating this research is a suggestion to refer specifically

to nationality. Furthermore, Indonesia is a culture-dominated country so it is advisable to be able to examine research models that have been proposed for broad-coverage and global acceptance of certain business orientations [36]. So it is recommended to conduct a longitudinal study using the proposed research model to be able to make decisions in long-term use. In the end, from these demographic variables produce moderate influences that have not been studied so that they can be taken into account, then for findings derived from demographic variables on actual use on mobile payments the QR-Code will produce and provide deeper knowledge.

REFERENCES

1. C.-W. Yap, **AliPay-Wechat Take Battle for Mobile Payment Dominance Overseas,** *The Wall Street Journal*, 2017. [Online]. Available: https://www.wsj.com/articles/alipay-wechat-take-battle-for-mobile-payment-dominance-overseas-1503144003. [Accessed: 12-Mar-2019].
2. H. Margianto, **Cashless Society Ketika Uang Fisik Hilang dari Dompet Anda,** *Kompas*, 2014. [Online]. Available: https://ekonomi.kompas.com/read/2014/08/30/2044448826/.Cashless.Society.Ketika.Uang.Fisik.Hilang.dari.Dompet.Anda. [Accessed: 11-May-2019].
3. **Indonesia's mobile payments industry to enter defining year,** *FT Confidential Research*, 2017. .
4. D. Setyowati, **Tren Baru Pembayaran Kode QR Yang Menyimpan Masalah,** *Kata Data*, 2019. [Online]. Available: https://katadata.co.id/berita/2018/09/11/tren-baru-pembayaran-kode-qr-yang-menyimpan-masalah. [Accessed: 11-May-2019].
5. J. Claessens, V. Dem, D. De Cock, B. Preneel, and J. Vandewalle, **"On the security of today's online electronic banking systems,"** *Comput. Secur.*, vol. 21, no. 3, pp. 253–265, 2002. https://doi.org/10.1016/S0167-4048(02)00312-7
6. T. Dahlberg, N. Mallat, J. Ondrus, and A. Zmijewska, **Past, present and future of mobile payments research: A literature review,** *Electron. Commer. Res. Appl.*, vol. 7, no. 2, pp. 165–181, 2008. https://doi.org/10.1016/j.elerap.2007.02.001
7. J. Donner and C. A. Tellez, **Mobile banking and economic development: Linking adoption, impact, and use,** *Asian J. Commun.*, vol. 18, no. 4, pp. 318–332, 2008. https://doi.org/10.1080/01292980802344190
8. A. F. Westin, **Privacy and freedom New York Atheneum, 1967,** *Priv. Pers. Rec. Civ. Lib. Rev. (Jan./Feb., 1976)*, pp. 28–34, 1967.
9. R. K. Chellappa and P. A. Pavlou, **Perceived information security, financial liability and consumer trust in electronic commerce transactions,** *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 358–368, 2002. https://doi.org/10.1108/09576050210447046
10. B. Shneiderman, **Designing trust into online experiences,** *Commun. ACM*, vol. 43, no. 12, pp. 57–59, 2000.
11. P. G. Schierz, O. Schilke, and B. W. Wirtz, **Understanding consumer acceptance of mobile payment services: An empirical analysis,** *Electron. Commer. Res. Appl.*, vol. 9, no. 3, pp. 209–216, 2010.
12. K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, **QR code security: A survey of attacks and challenges for usable security,** in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2014, pp. 79–90. https://doi.org/10.1007/978-3-319-07620-1_8
13. A. Bharambe, V. Bhirud, D. Bhuse, and C. Science, **Android Mobile Based Payment System Using QR Code,** vol. 3, no. 3, pp. 231–234, 2016.
14. F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, **User acceptance of computer technology: a comparison of two theoretical models,** *Manage. Sci.*, vol. 35, no. 8, pp. 982–1003, 1989.
15. M. Fishbein and I. Ajzen, ***Predicting and changing behavior: The reasoned action approach*.** Psychology press, 2011.
16. D. P. Y. Suseno and T. J. Yamada, **Two-dimensional, threshold-based cloud type classification using MTSAT data,** *Remote Sens. Lett.*, vol. 3, no. 8, pp. 737–746, 2012. https://doi.org/10.1080/2150704X.2012.698320
17. A. L. Mohmod, G. Krishnasamy, and M. I. Adenan, **Malaysian plants with potential in vitro trypanocidal activity,** *Ann. Phytomedicine*, vol. 4, no. 1, pp. 6–16, 2015.
18. V. Venkatesh and F. D. Davis, **A theoretical extension of the technology acceptance model: Four longitudinal field studies,** *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, 2000.
19. G. C. Moore and I. Benbasat, **Development of an instrument to measure the perceptions of adopting an information technology innovation,** *Inf. Syst. Res.*, vol. 2, no. 3, pp. 192–222, 1991.
20. Y. Chen and W. Salmanian**, User Acceptance in the Sharing Economy,** no. May, 2017.
21. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis**, User acceptance of information technology: Toward a unified view,** *MIS Q.*, pp. 425–478, 2003.
22. J. B. Rotter, **Interpersonal trust, trustworthiness, and gullibility.,** *Am. Psychol.*, vol. 35, no. 1, p. 1, 1980.
23. J. C. Anderson and J. A. Narus, **A model of distributor firm and manufacturer firm working partnerships,** *J. Mark.*, vol. 54, no. 1, pp. 42–58, 1990.
24. R. C. Mayer, J. H. Davis, and F. D. Schoorman, **An**

integrative model of organizational trust, *Acad. Manag. Rev.*, vol. 20, no. 3, pp. 709–734, 1995. https://doi.org/10.5465/amr.1995.9508080335

25. E. Desmayanti, **Faktor-Faktor yang Mempengaruhi Penggunaan Fasilitas E-Filling oleh Wajib Pajak sebagai Sarana Penyampaian SPT Masa secara Online dan Realtime (Kajian Empiris di Wilayah Kota Semarang),** Fakultas Ekonomika dan Bisnis, 2012.
26. B. Friedman, P. H. Khan Jr, and D. C. Howe, **"Trust online,"** *Commun. ACM*, vol. 43, no. 12, pp. 34–40, 2000.
27. D. J. Kim, D. L. Ferrin, and H. R. Rao, **A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents,** *Decis. Support Syst.*, vol. 44, no. 2, pp. 544–564, 2008. https://doi.org/10.1016/j.dss.2007.07.001
28. M. Hanafi, ***Manajemen Resiko***. Yogyakarta: Unit Penerbit dan Percetakan Sekolah Tinggi Ilmu Manajamen YKPN, 2006.
29. V. Swaminathan, E. Lepkowska-White, and B. P. Rao, **Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange,** *J. Comput. Commun.*, vol. 5, no. 2, p. JCMC523, 1999.
30. M. S. Featherman and P. A. Pavlou, **Predicting e-services adoption: a perceived risk facets perspective,** *Int. J. Hum. Comput. Stud.*, vol. 59, no. 4, pp. 451–474, 2003.
31. S. L. Jarvenpaa, N. Tractinsky, and L. Saarinen, **Consumer trust in an Internet store: A cross-cultural validation,** *J. Comput. Commun.*, vol. 5, no. 2, p. JCMC526, 1999.
32. W. D. Salisbury, R. A. Pearson, A. W. Pearson, and D. W. Miller, **Perceived security and World Wide Web purchase intention,** *Ind. Manag. Data Syst.*, vol. 101, no. 4, pp. 165–177, 2001.
33. F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, **Extrinsic and intrinsic motivation to use computers in the workplace 1,** *J. Appl. Soc. Psychol.*, vol. 22, no. 14, pp. 1111–1132, 1992.
34. Sugiyono, ***Metode Penelitian Kuantitatif. Kualitatif, dan R&D*.** Bandung: Alfabeta, 2010.
35. M. A. Mazurowski, P. A. Habas, J. M. Zurada, J. Y. Lo, J. A. Baker, and G. D. Tourassi, **Training neural network classifiers for medical decision making: The effects of imbalanced datasets on classification performance,** *Neural networks*, vol. 21, no. 2–3, pp. 427–436, 2008. https://doi.org/10.1016/j.neunet.2007.12.031
36. S. McCoy, D. F. Galletta, and W. R. King, **Applying TAM across cultures: the need for caution,** *Eur. J. Inf. Syst.*, vol. 16, no. 1, pp. 81–90, 2007.
37. V. Goyal, Dr.U.S. Pandey, and S. Batra. **Mobile Banking in India : Practices, Challenges, and Security Issues**, International Journal of Advanced Trends in Computer Science and Engineering, vol 1, No.2, May – June 2012, ISSN No. 2278 -3091.
38. E. Micheni, I. Lule, and G. Muketha. **Transaction Costs and Facilitating Conditions as Indicators of the Adoption of Mobile Money Services in Kenya,** International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), 9-15, 2013.