ILKOM Jurnal Ilmiah Vol. 14, No. 2, August 2022, pp. 91-98
Accredited 2nd by RISTEKBRIN No. 200/M/KPT/2020; E-ISSN 2548-7779 | P-ISSN 2087-1716

Factors influencing smartphone owners' acceptance of Biometric Authentication methods

La Ode Abdul Wahid [a,1]; Ahmad R Pratama [a,2*];
[a] *Universitas Islam Indonesia, Jl. Kaliurang No.Km. 14,5, Yogyakarta and 55584, Indonesia*
[1] *la.wahid@students.uii.ac.id;* [2] *ahmad.rafie@uii.ac.id;*
** Corresponding author*

Article history: Received February 21, 2022; Revised March 10, 2022; Accepted April 08, 2022; Available online August 30, 2022

Abstract

Smartphones are the world's most widely used personal computing devices. PINs and passcodes have long been the most popular authentication methods in smartphones and even in the pre-smartphone era. Due to the inconvenient nature of PINs and passcodes, a new biometric authentication method for smartphones was developed and has been gaining traction in terms of adoption, beginning with flagship devices and progressing to some mid-range devices. This article aims to investigate the factors influencing smartphone owners' acceptance of biometric authentication methods by developing a new model based on the Technology Acceptance Model (TAM). It also validates the data with survey data from 233 Indonesian smartphone owners via an online survey and analyzed it using Structural Equation Modeling (SEM). The results from the SEM analysis show that all nine hypotheses in the proposed model are supported. In other words, all six factors in the proposed model (i.e., attitude toward the use, perceived usefulness, perceived the ease of use, perceived enjoyment, perceived security, and social influence) have significant effects on the behavioral intention of adopting biometric authentication methods among smartphone owners. More specifically, the findings indicate that most Indonesian smartphone users have a favorable attitude toward biometric authentication, which is why they are willing to adopt it. Furthermore, it is discovered that the perceived usefulness of a biometric authentication method on smartphones outweighs its perceived ease of use. It reveals that the user's belief in the intrinsic value of biometric authentication methods in the form of perceived security outweighs both the internal user motivation of perceived enjoyment and the external user motivation of social influence in terms of their acceptance of biometric authentication methods.

Keywords: Authentication Method; Biometrics; Smartphone; Technology Acceptance; Structural Equation Modeling.

Introduction

With the widespread use of smartphones, users begin to be focus on the privacy and security of their data. The security of users' data is becoming increasingly important, particularly in terms of medical information, personal identification, social media, financial data, or other information obtained, as the data may be stolen, sold, or misused by identity thieves who are victims of cybercrime [1]–[3]. As a result, software vendors are increasingly competing to rely on various authentication types, typically just usernames, password conversions, or [4], [5]. Unfortunately, passwords as an authentication method have numerous security problems. The use of biometrics is one of the most promising options.

Biometric technology is the combination of biosensors, computer technology, and biostatistics. More specifically, human innate physical characteristics (such as the iris, face, fingerprints, palm prints, and so on) and behavioral characteristics (such as gait, voice notes, etc.). Fingerprint-based biometrics, the most widely used technique for identifying people, refers to the palm's texture, consisting of bumps, pinpoint dots, major lines, wrinkles, and single dots. With the advent of mature technology and low cost, fingerprinting has become the preferred option, particularly in commercial applications. Because the face is the most natural biometric feature that can be used to recognize fellow beings, it is the most natural biometric feature that utilizes spatial parameters such as gender, beard, edge map, and pixel intensity.

Several previous studies attempted to understand how users interact with their mobile devices. Many smartphone users use their devices to manage personal information and private communications. Using such devices creates a symbiotic relationship between the user and his smartphone. With the advancement of the mobile internet, an increasing number of applications are being used on smartphones [6]. Many rely on smartphones to conduct sensitive applications and transactions [7], [8]. Unauthorized users, for example, can steal smartphones and gain access to

http://dx.doi.org/10.33096/ilkom.v14i2.1114.91-98

photos, contacts, and even bank accounts. As a result, authentication methods are critical for preventing unauthorized users from gaining access. The most common approaches are non-transparent methods (e.g., passwords and PINs). This method, however, necessitates a user-aware interaction and a predefined secret, which an attacker can quickly discover.

Furthermore, even in place, this method does not always prevent malicious users from gaining access to the phone, for example, by answering incoming calls [9]. As a result, researchers are concentrating their efforts on developing authentication methods that are more precise, useful, and less vulnerable to attackers. The biometric authentication method analyzes humans using physiological characteristics (such as the face [5], [7], [8], fingerprints [10], [11], and iris [5]) and human traits or behavior (such as keystroke and gait) [12].

As the number of smartphone users who use biometric security systems grows, this study will examine why some smartphone users do not use this biometric system for authentication. Researchers also want to investigate the real-world effects of these systems in controlled environments and everyday life. In particular, examining the user's expectations of the system's dependability and usability. We employed an online survey to collect data on the usefulness of this scheme, as well as user perceptions and attitudes toward the project and adopting the TAM (Technology Acceptance Model) method by adding some new constructs. The data will then be processed and analyzed using the SEM (Structural Equation Modeling) method to determine the relationship between the exogenous latent variables and the endogenous latent variable, which is their intention to use biometric authentication methods [13].

Method

A. Data Collection

This study's population and sample were Indonesian smartphone users. Data is collected by filling out online questionnaires independently through Google Forms so that they can be accessed by the prospective respondents at any time and from any location. The questionnaires were distributed online from November 4th, 2020, to June 20th, 2021. In total, 233 respondents provided demographic information, as shown in **Table 1**.

Table 1. Demographic Information of Participants

Charactistics	Category	N	%
Sex	Male	106	45.49%
	Female	127	54.51%
Age	11-25	159	68.24%
	26-35	50	21.46%
	> 35	24	10.30%
Location	Java	184	78.97 %
	Outside Java	49	21.03%
Occupations	Unemployed	93	39.91%
	Public sector	49	21.03%
	Private sector	65	27.90%
	Freelance	26	11.16%
Education	Up to high school	109	46.78%
	College degree	124	53.22%
Mobile Devices	iOS	184	78.97%
	Android	49	2103%
Total		233	100.00%

B. Data Analisys

The SEM (Structural Equation Modeling) method was used for data analysis in this study, which was analyzed through the R programming language and R studio software and Lavaan library [14], [15]. Structural equation modeling (SEM) is a statistical technique for developing and testing statistical models, which are typically in the form of a model of the relationship between endogenous variables (effect) and exogenous variables (cause), which has been used in many studies on mobile technology acceptance [16], including m-learning [17] and m-commerce [18] among others. According to Sarwono [19], SEM outperforms Multiple Regression Analysis, Path Analysis, Factor Analysis, Time Series Analysis, and Covariance Analysis because it takes into account interaction modeling, nonlinearity, correlated independents, measurement errors, correlated error terms, and multiple latent independents, each of which is measured using a different number of indicators and variables depending on the indicator.

C. Tecnology Acceptance Model

Several frameworks have been developed in the Information Technology and Information System literature to explain the use of innovation [19], including the Theory of Reasoned Action (TRA), Technology Acceptance Model

(TAM), Theory of Planned Behavior (TPB), Decomposed Theory of Planned Behavior (DTPB), and Unified Theory of Acceptance and Use of Technology (UTAUT). Among them, TAM is considered as the most influential and is generally used to explain the individual acceptance of the use of information technology systems [13]. In addition, the TAM proposed by Davis [20] has grown to be the most popular one because it is considered as the most influential extension of TRA, replacing variables related to attitudes and behavior control with technology acceptance measures. TAM was first introduced by Davis [13] in 1986 to determine computer usage behavior. TAM is a theoretical framework specifically designed to help analyze and predict the tendency of users to accept new information technology [21]. The original constructs of TAM consisted of [20]:

1) Perceived usefulness (PU) refers to the belief that using a particular system will improve one's performance [7]. PU is more significant and important than other variables in influencing attitudes, behavioral intentions, and behavior in using technology [22].

2) Perceived ease of use (PEOU) is defined as a person's belief that using a particular system will be simple, easy, and requires little to no effort.

3) Attitude towards using technology (ATT) is defined as positive or negative feelings from someone if they have to perform the specified behavior. Jogiyanto [23] concludes, based on the results of previous studies, that attitude can positively affect behavioral intention. Still, several other studies have also shown that attitude does not significantly affect behavioral intention. As a result, some TAM studies do not include this attitude variable in the model.

4) Behavioral intention (BI) is the intention to use technology and the behavioral tendency to continue applying or using it. This variable is the endogenous variable, and in many studies employing TAM, it represents the actual system use that is not directly measured.

In addition to the four original constructs, this study introduces some new constructs based on what has been learned from the literature and additional considerations about the type of technology whose adoption or acceptance is being measured. This research adds three new constructs to the model, including:

1) Perceived Security (PS). The biometric authentication system is not perfect. It is still susceptible to various attacks, including replay/forgery attacks. However, it is essential to see if users see it as a more secure authentication method, which can be a legitimate reason to adopt it.

2) Perceived Enjoyment (PE). When used in public, biometric authentication methods can make smartphones appear to be more stylish, especially in developing countries where there are still many entry-level smartphones on the market that do not support biometrics. In this regard, this may be one of the factors driving biometric adoption among Indonesian smartphone users.

3) Social Influence (SI). It is undeniable that some users believe they should use certain technologies because other influential people have done so (e.g., family, relatives, and friends). Even more so in collectivist countries such as Indonesia. It is, therefore, understandable that SI is one of the factors driving the adoption of biometric authentication technology.

Considering all the original and new constructs, **Figure 1** and **Table 2** illustrate the hypothesized relationships between them. At the same time, **Table 3** summarizes the measurement items for all latent variables in this study.

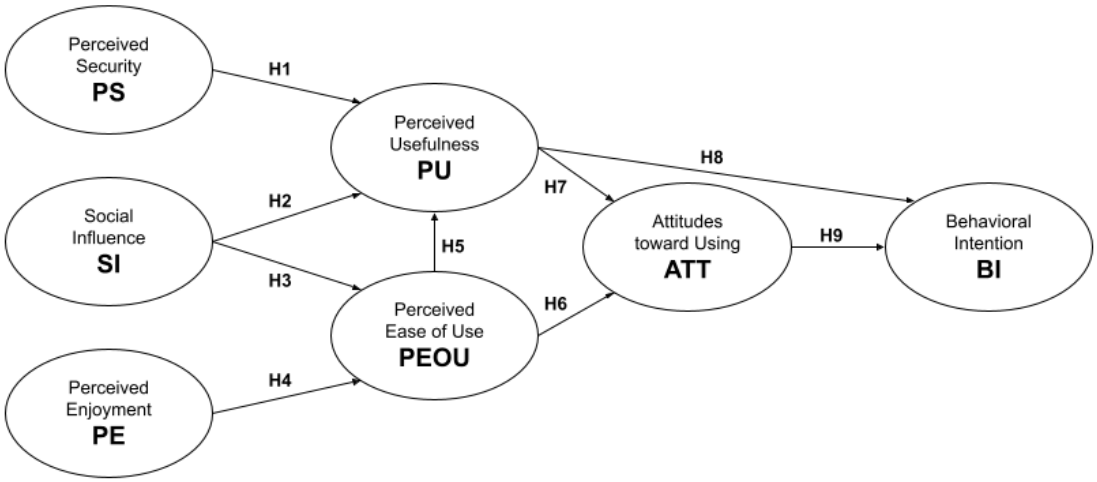


Figure 1. The proposed model in this study

Table 2. List of Hypotheses in this study

Code	Relationship	Description
H1	PS → PU	Higher level of perceived security increases perceived usefulness of biometric authentication methods
H2	SI → PU	Stronger social influence increases perceived usefulness of biometric authentication methods
H3	SI → PEOU	Stronger social influence increases perceived ease of use of biometric authentication methods
H4	PE → PEOU	Higher level of perceived enjoyment increases perceived ease of use of biometric authentication methods
H5	PEOU → PU	Higher level of perceived ease of use increases perceived usefulness of biometric authentication methods
H6	PEOU → ATT	Higher level of perceived ease of use increases positive attitudes toward biometric authentication methods
H7	PU → ATT	Higher level of perceived usefulness increases positive attitudes toward biometric authentication methods
H8	PU → BI	Higher level of perceived usefulness increases behavioral intention of using biometric authentication methods
H9	ATT → BI	Higher level of positive attitudes toward biometric authentication methods increases behavioral intention of using them

Table 3. Variables and Measurement Items

Variables	Code	Measurement Items
Original TAM Constructs	pu1	Biometrics makes unlocking the phone lock screen easier
	pu2	Biometrics makes unlocking the phone lock screen faster
	pu3	Biometrics makes unlocking the phone lock screen more secure
	pu4	In general, biometric authentication methods provide many benefits
	peou1	I can easily master how to use the biometric authentication method
	peou2	I don't have to spend a lot of time and effort when using biometric authentication methods
	peou3	I can easily find the information I need to use the biometric authentication method
	att1	I have a positive assessment of the existence of a biometric authentication method
	att2	In my opinion, a biometric authentication method is something that is necessary
	att3	I like to use biometric authentication method
	bi1	I use the biometric authentication method voluntarily without coercion from anyone
	bi2	I prefer to use biometric rather than pin, password, or pattern based authentication methods
	bi3	I intend to continue using the biometric authentication method
New Constructs in This Study	ps1	The biometric authentication method is more secure than using a password, pin or pattern to unlock the phone lock screen
	ps2	The technology used in the biometric authentication provides security guarantees for me
	ps3	In general, I feel safe using the service of the biometric authentication method
	pe1	Using biometric authentication methods is something that I enjoy
	pe2	Using biometric authentication methods is an interesting thing for me
	pe3	Using biometric authentication methods can increase my prestige and self-esteem
	pe4	I use the biometric authentication method because it fits my lifestyle
	si1	My family members also use biometric authentication methods
	si2	My close friends also use the biometric authentication method
	si3	My colleagues (coworkers, classmates, etc.) also use biometric authentication methods
	si4	Many other people I have met are also using biometric authentication methods

Results and Discussion

The loadings factor from Confirmatory Factor Analysis (CFA) is examined to determine the model's validity, as shown in **Table 4**. One item, i.e., pe3, was omitted from the SEM analysis because its loading score is less than 0.7 [24]. Next, the discriminant validity test examined the correlation between variables, known as the Heterotrait-Monotrait ratio (HTMT). A correlation value that greater than 0.9 indicates poor discriminant validity [25], [26]. **Table 5** shows two HTMT values above 0.9, but both are found in the original TAM construct relationships, including PU-PEOU and ATT-BI, so they are quite safe to ignore. Furthermore, as shown in **Table 4**, several goodness-of-fit indices indicate an excellent fit between the data and the proposed model in this study.

Once all the previous tests were passed, the SEM was run with all measurement items treated as categorical instead of numerical. The standardized path coefficients were retrieved along with their respective p-values to

indicate whether or not the hypothesized relationship was statistically significant. **Figure 2** summarizes the findings of this path analysis.

Table 4. Mean, Standard Deviation, and Loading Scores

No.	Item	Mean	SD	Loadings
1	pu1	3.738	1.08	0.899
2	pu2	3.807	1.08	0.885
3	pu3	3.639	1.08	0.833
4	pu4	3.627	1.00	0.900
5	peou1	3.601	0.94	0.908
6	peou2	3.639	1.07	0.904
7	peou3	3.536	0.97	0.865
8	si1	3.133	0.92	0.769
9	si2	3.382	0.96	0.926
10	si3	3.421	0.93	0.948
11	si4	3.429	0.97	0.914
12	ps1	3.416	1.12	0.901
13	ps2	3.455	1.06	0.955
14	ps3	3.511	1.00	0.929
15	pe1	3.498	1.02	0.947
16	pe2	3.571	1.01	0.929
17	pe3*	3.004	1.09	0.604
18	pe4	3.163	1.11	0.784
19	atu1	3.609	0.99	0.907
20	atu2	3.678	1.01	0.924
21	atu3	3.571	1.05	0.947
22	biu1	3.700	1.06	0.901
23	biu2	3.356	1.08	0.854
24	biu3	3.421	1.07	0.903

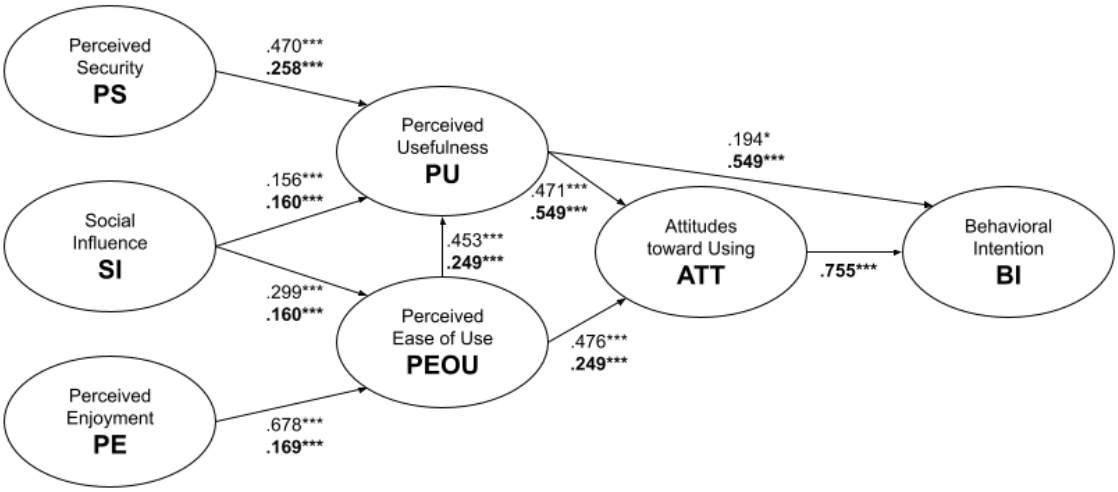
Note: *item omitted from the SEM due to low loading score

Table 5. Heterotrait-monotrait ratio

Factor	PU	PEOU	SI	PS	PE	ATT	BI
PU	1.000						
PEOU	0.926	1.000					
SI	0.818	0.793	1.000				
PS	0.860	0.727	0.640	1.000			
PE	0.889	0.867	0.783	0.797	1.000		
ATT	0.915	0.883	0.788	0.747	0.898	1.000	
BI	0.866	0.836	0.764	0.774	0.883	0.926	1.000

Table 6. Goodness of fit indices

Index	Value	Recommended Threshold	Verdict
χ^2/df	2.268	< 3.00 [27]	Excellent Fit
SRMR	0.04	< 0.08 [28]	Excellent Fit
RMSEA	0.07	< 0.08 [29]	Excellent Fit
CFI	0.99	> 0.95 [28]	Excellent Fit
TLI	0.99	> 0.95 [30]	Excellent Fit



Note: Numbers reported are standardized coefficient of direct effect between the two variables connected by the straight line with the total effect of the exogeneous variable on the ultimate endogeneous variable (BI) at the bottom in bold. * p < 0,5; ** p < 0,01; *** p < 0,001

Figure 2. Path coefficients of the model based on the SEM results

Furthermore, to determine the magnitude of each factor's effect on BI, the total effects were compared by adding the direct and indirect effects as shown in **Table 7**.

Table 7. Standardized estimates of each exogenous variable on bi

Relationship	Standardized Estimates		
	Direct Effect	***Indirect Effect***	***Total Effect***
PS → BI	-	0.258 ***	0.258 ***
SI → BI	-	0.160 ***	0.160 ***
PE → BI	-	0.169 ***	0.169 ***
PEOU → BI	-	0.249 ***	0.249 ***
PU → BI	0.194 *	0.355 ***	0.549 ***
ATT → BI	0.865 ***	-	0.755 ***

Finally, the summary of all hypothesis tests is presented in **Table 8**. All nine hypotheses in this study (H1, H2, H3, H4, H5, H6, H7, H8, and H9) are directly supported. In other words, these three additional models significantly affect smartphone users' acceptance of biometric authentication methods. Furthermore, based on the total effects summarized in **Table 7**, PU is more important than PEOU in biometric authentication method adoption in Indonesia. This finding is quite similar to that of many other technology acceptance studies employing TAM, including the original one. As for the new constructs added to the model in this study, PE is apparently slightly more important than SI, but PS is significantly more important than both in driving user acceptance of biometric authentication methods in Indonesia. In other words, one of the main reasons smartphone users in Indonesia adopt biometric authentication methods is because they believe it can help secure their smartphones, including accounts and data stored in them. This is an exciting finding since some smartphone users will only adopt a new security measure when they have something to lose [31].

Table 8. Summary of Hypotheshes Tesis

Hypothesis	Relationship	Status
H1	PS → PU	Supported
H2	SI → PU	Supported
H3	SI → PEOU	Supported
H4	PE → PEOU	Supported
H5	PEOU → PU	Supported
H6	PEOU → ATT	Supported
H7	PU → ATT	Supported
H8	PU → BI	Supported
H9	ATT → BI	Supported

Conclusion

This study proposed an acceptance model of the biometric authentication method among Indonesian smartphone users. The model was developed from TAM by adding three new constructs to represent the technology (PS), the internal motivation of users (PE), and the external motivation of the users (SI). As it turns out, of all three, PS has the highest effect in driving users' acceptance of biometric authentication. In other words, many Indonesian smartphone users choose to use the biometric authentication method because they believe in the security feature of biometric authentication compared to any other authentication methods on smartphones. In addition, for some smartphone users, using biometric authentication methods enable them to feel and look good in front of the public because they see more people around them who are also using them. Moreover, it also found that most Indonesian smartphone users know the usefulness of biometric authentication as a better reason to adopt it than its ease of use. Finally, most Indonesian smartphone users hold positive attitudes toward the biometric authentication method, which is the main reason behind their willingness to adopt this technology.

References

[1] M. R. Ramadhani and A. R. Pratama, "Analisis kesadaran cybersecurity pada pengguna media sosial di Indonesia," *journal.uii.ac.id*, vol. 1, no. 2, pp. 1–8, 2020.

[2] M. S. Alif and A. R. Pratama, "Analisis kesadaran keamanan di kalangan pengguna E-Wallet di Indonesia," *AUTOMATA*, vol. 2, no. 1, 2021.

[3] M. R. Akhyari and A. R. I. Pratama, "Kesadaran akan ancaman serangan berbasis backdoor di kalangan pengguna smartphone android," *AUTOMATA*, vol. 2, no. 1, 2021.

[4] D. Kunda and M. Chishimba, "A survey of android mobile phone authentication schemes," *Mob. Netw. Appl.*, vol. 26, no. 6, pp. 2558–2566, Dec. 2021.

[5] A. Hadid, J. Y. Heikkila, O. Silven, and M. Pietikainen, "Face and eye detection for person authentication in mobile phones," in *2007 First ACM/IEEE International Conference on Distributed Smart Cameras*, Vienna, Austria, 2007.

[6] Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu, and X. Zhou, "BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics," *Ad Hoc Netw.*, vol. 84, pp. 9–18, Mar. 2019.

[7] A. Rattani and R. Derakhshani, "A survey of mobile face biometrics," *Comput. Electr. Eng.*, vol. 72, pp. 39–52, Nov. 2018.

[8] A. Choudhary and R. Vig, "Mobile biometrics using Face Recognition," in *Communication and Computing Systems*, Dronacharya College of Engineering, Gurgaon, India, 2016.

[9] M. Conti, I. Zachia-Zlatea, and B. Crispo, "Mind how you answer me!," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11*, Hong Kong, China, 2011.

[10] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, "Mobile device identification via sensor fingerprinting," *arXiv [cs.CR]*, 06-Aug-2014.

[11] D. Afah, A. Gautam, S. Misra, A. Agrawal, R. Damaševičius, and R. Maskeliūnas, "Smartphones verification and identification by the use of fingerprint," in *Advanced Techniques for IoT Applications*, Singapore: Springer Singapore, 2022, pp. 365–373.

[12] A. K. Jain, P. Flynn, and A. A. Ross, Eds., *Handbook of biometrics*. New York, NY: Springer, 2010.

[13] 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, Aug. 1989.

[14] RStudio Team(2015), "RStudio: Integrated Development for R," *RStudio, Inc., Boston, MA*, p. http://www.rstudio.com/., 2015.

[15] Y. Rosseel, "lavaan : An R Package for Structural Equation Modeling," *Journal of Statistical Software*, vol. 48, no. 2, pp. 1–36, 2012.

[16] M. Abad, I. Díaz, and M. Vigo, "Acceptance of mobile technology in hedonic scenarios," in *Proceedings of the 2010 British Computer Society Conference on Human-Computer Interaction, BCS-HCI 2010*, 2010, pp. 250–258.

[17] A. R. Pratama, "Fun first, useful later: Mobile learning acceptance among secondary school students in Indonesia," *Education and Information Technologies*, vol. 26, no. 2, pp. 1737–1753, Mar. 2021.

[18] S.-C. Chang, C.-C. Sun, L.-Y. Pan, and M.-Y. Wang, "An extended TAM to explore behavioural intention of consumers to use M-Commerce," *Journal of Information & Knowledge Management*, vol. 14, no. 02, p. 1550014, Jun. 2015.

[19] Y. Sarwono, "Pengertian dasar Structural Equation Modeling (SEM)," *Jurnal Ilmiah Manajemen Bisnis Ukrida*, vol. 10, no. 3, p. 98528, 2010.

[20] P. G. Schierz, O. Schilke, and B. W. Wirtz, "Understanding consumer acceptance of mobile payment services: an empirical analysis," *Electronic Commerce Research and Applications*, vol. 9, no. 3, pp. 209–216, 2010.

[21] W. Widiyanti, "Pengaruh kemanfaatan, kemudahan penggunaan dan promosi terhadap keputusan penggunaan E-Wallet OVO di Depok," *Moneter - Jurnal Akuntansi dan Keuangan*, vol. 7, no. 1, pp. 54–68, 2020.

[22] M. Conti, I. Zachia-Zlatea, and B. Crispo, "Mind how you answer me!: (Transparently authenticating the user of a smartphone when answering or placing a call)," *Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011*, pp. 249–260, 2011.

[23] H. M. Jogiyanto, *Sistem Informasi Keperilakuan*. Yogyakarta: Andi Offset, 2007.

[24] C. Fornell and D. F. Larcker, "Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and.pdf," *Journal of Marketing Research*, vol. XVIII, no. February, pp. 39–50, 1981.

[25] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, vol. 43, no. 1, pp. 115–135, Jan. 2015.

[26] G. Franke and M. Sarstedt, "Heuristics versus statistics in discriminant validity testing: a comparison of four procedures," *Internet Research*, vol. 29, no. 3, pp. 430–447, 2019.

[27] R. B. Kline, "Principles and practice of structural equation modeling," 2015.

[28] L. T. Hu and P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling*, vol. 6, no. 1, pp. 1–55, 1999.

[29] R. C. MacCallum, M. W. Browne, and H. M. Sugawara, "Power analysis and determination of sample size for covariance structure modeling," *Psychological Methods*, vol. 1, no. 2, pp. 130–149, 1996.

[30] D. Hooper, J. Coughlan, M. R. Mullen, and E. T. Al., "Evaluating model fit : a Synthesis of the Structural Equation Modelling Literature," *Electronic Journal of business Research Methods*, vol. 6, no. 1, pp. 53–60, 2008.

[31] A. R. Pratama and F. M. Firmansyah, "Until you have something to lose! Loss aversion and two-factor authentication adoption," *Applied Computing and Informatics*, vol. ahead-of-print, no. ahead-of-print, pp. 1–12, Jan. 2021.