The Indonesian Journal of Computer Science
www.ijcs.net
Volume 15, Issue 2, April 2026
https://doi.org/10.33022/ijcs.v15i2.5091

Factors Influencing the Adoption of Multi Factor Authentication in the Public Sector: A Case Study of Indonesia National Single Window Agency

Dencaswo Purnomo[1], Amanda Ghaisani [2], Dana Indra Sensuse [3], Sofian Lusa [4], Nurcholis Ramlan[5], Nur Indrawati [6]
dencaswo.purnomo@ui.ac.id[1], amanda.ghaisani41@ui.ac.id[2], dana@ui.ac.id[3], sofian.lusa@iptrisakti.ac.id[4], nurholis.ramlan@ui.ac.id[5], nur.indrawati21@ui.ac.id[6]
[1,2,3,5,6] Faculty of Computer Science, University of Indonesia
[4] Faculty of Tourism, Trisakti Institute of Tourism

Article Information

Received : 20 Feb 2026
Revised : 18 Mar 2026
Accepted : 25 Mar 2026

Keywords

Multi Factor Authentication, TAM, UTAUT, Perceived Security, Indonesia National Single Window Agency

Abstract

This study aims to examine the factors that influence the intention and actual use of Multi-Factor Authentication (MFA) in the National Single Window Agency (LNSW). The research model integrates the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) with the addition of the Perceived Security (PS) construct. Data were collected from employees and vendor teams at the LNSW and analyzed using the Partial Least Squares Structural Equation Modeling (PLS-SEM) method. The results show that Perceived Ease of Use (PEOU) and Social Influence (SI) have a positive and significant effect on Behavioral Intention (BI). In addition, Perceived Security (PS) does not have a direct effect on Behavioral Intention, but it has a significant positive effect on Perceived Usefulness (PU). Other findings show that Behavioral Intention (BI) is a strong predictor of Actual Usage (AU) of MFA. These results confirm the relevance of the TAM and UTAUT models in explaining the adoption of security technology in the public sector, and emphasize the importance of ease of use and organizational influence in encouraging the adoption of MFA.

A. Introduction

Advances in digital transformation in the public sector have prompted the government to improve information security systems, particularly the exchange of electronic data related to exports, imports, and logistics between ministries and agencies in Indonesia, as well as across countries in the context of international trade [1], [2]. The Indonesia National Single Window Agency (LNSW) as the organization that manages the Indonesia National Single Window System (SINSW) has an obligation to ensure system security, particularly confidentiality, integrity, and availability [1], [3], [4], [5]. Based on data from the Indonesia National Cyber and Crypto Agency (BSSN) during 2024, data theft and illegal data access were the most frequent security incidents in Indonesia. There were 22 reported cases [6]. The public sector was the most affected organization, accounting for 58.34%. This shows that government organizations are the main targets of cyber attacks [6]. In addition, 56 million pieces of data from 461 public organizations were leaked due to credential theft by malware. The data was used by attackers to conduct phishing and gain illegal access to public service systems [6]. This situation highlights the government's weak ability to protect credentials and the urgency of implementing Multi-Factor Authentication (MFA) in order to protect sensitive data in the public sector.

LNSW implements Multi-Factor Authentication (MFA) as a mandatory mechanism for all employees and vendors when accessing SINSW through Single Sign-On (SSO). This policy is established through a top-down approach, originating directly from top management. This policy has impacted system operations at LNSW. Many employees are not yet familiar with the MFA feature, causing various obstacles when logging into the system. These obstacles are due to the lack of change management in the implementation of MFA, such as training and the preparation of technical guidelines for using MFA, as well as low awareness of the importance of implementing MFA.

In addition, existing research on MFA adoption is limited to certain sectors such as the financial sector and the private sector. Currently, there is no empirical evidence examining MFA adoption in the public sector in Indonesia, particularly with organizations involving multiple stakeholders such as LNSW.

Based on these conditions, this study aims to identify the factors that influence the implementation of MFA at LNSW. The author uses a combined model of the Technology Acceptance Model (TAM) [7], [8] and the Unified Theory of Acceptance and Use of Technology (UTAUT) [9], [10], [11], and adds the construct of Perceived Security [12], [13]. The research question of this study is: What factors influence the implementation of MFA at LNSW?

Theoretically, this research contributes to the development of a system security adoption model by integrating user behavior and security perceptions. Practically, the results of this research are expected to serve as a reference for LNSW in formulating more adaptive and user-oriented security policies.

B. Related Theory

B.1. Basic Theory

MFA is an authentication mechanism that verifies users using two or more independent authentication factors, namely something you know (e.g., password or

PIN), something you have (e.g., token or physical device), and something you are (e.g., biometrics)[14], [15], [16].

The adoption of MFA in an organization can be measured using existing adoption theories, namely TAM [7] and UTAUT [9]. In this case study, the author adopted two constructs from the TAM model, namely Perceived Usefulness (PU), which explains users' perceptions that the implementation of MFA can increase the usefulness of the system [7], [8], [15], [16] and Perceived Ease of Use (PEOU), which describes users' perceptions of the extent to which MFA features are easy to use [7], [15], [17], [18], [19]. Meanwhile, from the UTAUT model, the author uses two constructs, namely Social Influence (SI) and Facilitating Conditions (FC). SI explains the extent to which social influences, such as superiors and coworkers, encourage users to use MFA[9], [10] and FC explains the extent to which the facilities perceived by users support the use of MFA [9], [10]. Both models play an important role in explaining the constructs of Behavioral Intention (BI) and Actual Usage (AU). BI explains users' intentions in using MFA [7], [9], while AU explains how MFA is actually used in organizations [7], [9].

In the context of MFA implementation, the author also uses the construct of Perceived Security (PS). PS describes users' perceptions of security and the organization's ability to protect data from security threats [8], [12], [13]. In several previous studies, MFA adoption was influenced by mandatory policies, usability, and user readiness [11], [15]. In Indonesia itself, there has been no research specifically examining the factors that influence MFA adoption, particularly in the public sector

B.2. Research Hypothesis

Figure 1. shows the eight hypotheses used in this study.

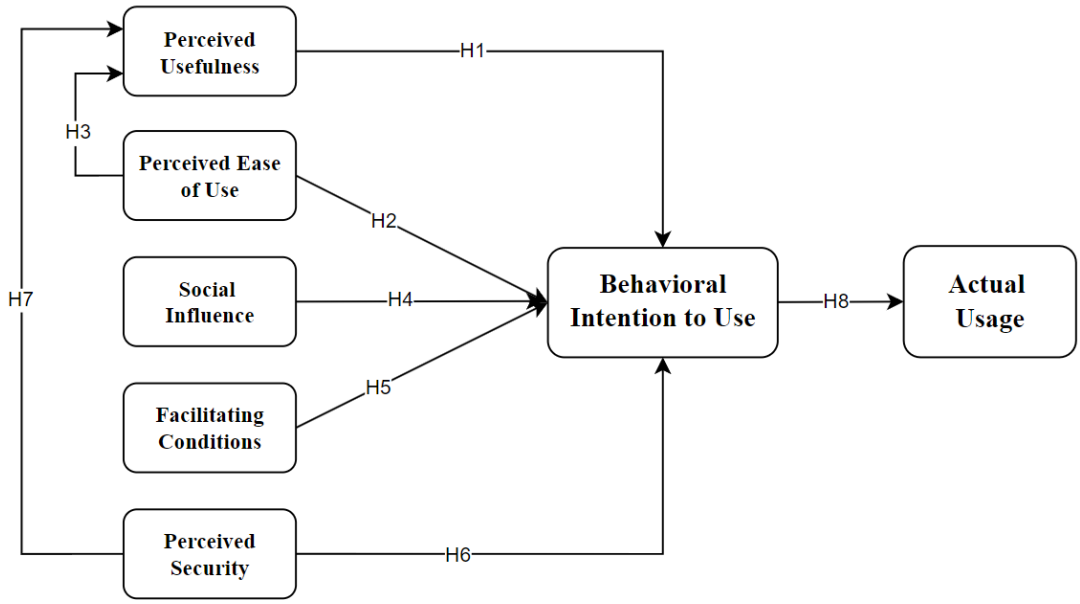

Figure 1. Research Model

Hypotheses H1, H2, and H3 adopt the basic TAM framework [7]. H1 (PU → BI) explains that the PU construct has a positive effect on BI in the implementation of MFA. In the context of digital security, mobile banking users tend to use biometric authentication when they perceive an increase in benefits [8], [12]. Meanwhile, H2

(PEOU → BI) and H3 (PEOU → PU) explain that system ease of use has a positive effect on users' intention to use MFA [7], [8], [15], and that an easy-to-use system will be considered more useful by users [7], [8]. Research by Azhari et al.[8] shows that the ease of use of biometric technology increases user acceptance in Indonesia, while Sinigaglia et al. [15] emphasize that the ease of authentication procedures is a major factor in the adoption of MFA in the banking sector.

Hypotheses H4 and H5 refer to the UTAUT framework [9]. H4 (SI → BI) explains that social influence has a positive impact on users' willingness to use MFA [9], [17] and H5 (FC → BI) explains that resource availability, technical support, and organizational infrastructure readiness have a positive effect on employees' intention to use MFA[9], [17]. Al Husari et al. [17] also states that adequate facilitating conditions are an important prerequisite for shaping employees' intention to adopt MFA.

Hypotheses H6 and H7 are related to PS. H6 (PS → BI) states that Perceived Security has a positive effect on Behavioral Intention. Perceived security is one of the strongest factors in determining employees' willingness to use digital services [12], [13]. In addition, H7 (PS → PU) states that perceived security has a positive effect on perceived usefulness [12], [13]. A sense of security in using the system makes users tend to view the system as useful [8].

Hypothesis H8 (BI → AU) states that Behavioral Intention has a positive effect on Actual Usage. In the TAM model [7], it is stated that user intention is a direct predictor of actual usage of a system because it reflects an individual's readiness to take concrete action [7]. This finding was then reinforced and developed in the UTAUT study by Venkatesh et al. [9].

C. Research Method

The stages in this research are arranged systematically as shown in Figure 2.

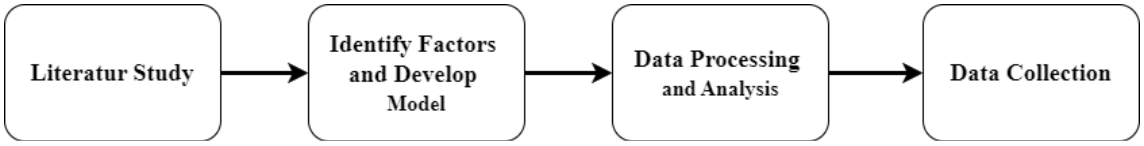

Figure 2. Research Stages

C.1. Literature Study

A literature study was conducted to identify factors that influence MFA adoption based on technology adoption theory and information system security. The results of the literature review were used as the basis for developing a conceptual model and formulating research variables.

C.2. Identify Factors and Develop Model

Based on the results of the literature review, this study identified seven main constructs that influence MFA adoption, namely PU and PEOU (TAM), SI and FC (UTAUT), PS (system security), and BI and AU as variables that influence users' willingness to use MFA

C.3. Data Collection

Data collection was conducted through a survey using a closed questionnaire with a 5-point Likert scale. Respondents consisted of LNSW employees and vendor teams who had used the MFA feature on the INSW System at least once in the past month. Respondents were selected using purposive sampling, involving functional roles related to information system development and operations.

C.4. Data Processing and Analyzing

Data analysis was performed using the Partial Least Squares Structural Equation Modeling (PLS-SEM) method with the assistance of SmartPLS software. Outer model evaluation was conducted to assess construct reliability and validity through outer loading values, Cronbach's Alpha, Composite Reliability (CR), and Average Variance Extracted (AVE), as well as discriminant validity using the Fornell–Larcker criteria [14], [15], [16].

Furthermore, the inner model was tested to analyze the relationship between constructs and hypothesis testing using the bootstrapping technique, including testing the direct and indirect effects on the BI construct [16].

D. Result

This section explains the research results, which consist of research respondent data and research data processing using PLS SEM.

D.1. Respondent Demographics and Behaviours

The following table presents the demographic details of the research respondents:

Table 1. Respondent Demographics

Category	Sub- Category	No of Participants	Percentage
Team Origin	Vendor Team	62	62%
	Internal LNSW Team	38	38%
Gender	Male	94	94%
	Female	6	6%
Roles	Programmer	5	13%
	Infrastructure and Information Security Team	10	26%
	PMO/Governance Team	1	3%
	Operations Team	12	32%
	System Analyst	4	11%
	Call Center/ Service Desk	3	8%
	Planning/IT Architect Team	3	8%

Based on the demographic information of the respondents, 100 participants were involved in this study, consisting of 62 respondents (62%) from the vendor team and 38 respondents (38%) from the internal IT team. The majority of respondents are male (94%), while only 6% are female. Most respondents were operations teams (32%), followed by infrastructure and information security teams (26%), programmers (13%), system analyst (11%), call center and IT planning/ architectural teams (8%), and PMO/Governance Team (8%). Table 2 illustrates the behavior details of the participants in the study

Table 2. Respondent Behaviors

Behavior		No of Participants	Percentage
Login frequency (per week)	< 3 times	28	28%
	> 10 times	28	28%
	3 to 5 times	34	34%
	5 to 10 times	10	10%
Most used feature	Tools Authenticator	51	51%
	OTP	7	7%
	PassKeys	42	42%

Based on behavior, the most respondents logged in during the week, between 3 to 5 times. Meanwhile, at least respondents log in 5 to 10 times a week. In addition, as many as 51% of respondents most often use Authenticator Tools such as Google Authenticator, Microsoft Authenticator, and the least use email OTP, which is 7%. This data is sufficient to present an overview of the respondents' backgrounds and behaviors regarding MFA usage within LNSW.

D.2. Measurement Model Assessment

The next step is to conduct an analysis by evaluating the measurement model. This evaluation consists of three aspects, namely discriminant validity, convergent validity, and internal consistency. [20].

Discriminant Validity

Discriminant validity is used to see whether one construct differs from another. This study uses the Fornell–Larcker criteria, which is one of the most widely accepted approaches in PLS-SEM analysis, particularly for exploratory research [21] [22]. Table 3 shows the results of Fornell Larcker.

Table 3. Discriminant Validity Fornell Larcker

	AU	BI	FC	PEOU	PS	PU	SI
AU	0.840						
BI	0.760	0.919					
FC	0.746	0.680	0.827				
PEOU	0.668	0.621	0.749	0.821			
PS	0.600	0.620	0.667	0.464	0.867		
PU	0.579	0.750	0.734	0.546	0.695	0.861	
SI	0.689	0.760	0.711	0.563	0.571	0.716	0.897

Indicator and Convergent Validity

Convergent validity is used to see whether each construct correlates with one another [23]. Convergent validity was evaluated using the Average Variance Extracted (AVE), with a threshold value of 0.500 [23]. The results of the analysis using smartPLS show that all constructs have met the required AVE threshold, as shown in Table 4.

Table 4. Validity And Reliability Testing

Indicator	Loading	Cronbach's Alpha	Composite Reliability (rho_c)	AVE
PU1	0.855	0.883	0.919	0.741

Indicator	Loading	Cronbach's Alpha	Composite Reliability (rho_c)	AVE
PU2	0.851	0.838	0.896	0.674
PU3	0.810			
PU4	0.923			
PEOU1	0.729			
PEOU2	0.912			
PEOU3	0.782			
PEOU4	0.848			
SI1	0.925	0.762	0.892	0.805
SI3	0.870			
FC1	0.761	0.846	0.896	0.684
FC2	0.797			
FC3	0.836			
FC4	0.908			
PS1	0.857	0.840	0.901	0.751
PS3	0.871			
PS4	0.872			
BI1	0.927	0.817	0.916	0.845
BI3	0.911			
AU1	0.801	0.793	0.878	0.706
AU2	0.801			
AU3	0.913			

Table 4 shows that all constructs have values above 0.500, which means that all constructs are valid. However, three indicators were removed from the model, the first is SI2 due to a loading value below the 0.700 threshold. The other two indicators are PS2 (0.952) and BI2 (0.958), which indicate redundancy within the measurement model [23], [24].

Internal Consistency/Reliability Testing

Internal consistency between indicators is measured using Cronbach's Alpha (Alpha) and Composite Reliability (CR) methods [23]. The results in Table 4 show that all constructs have met the required internal consistency criteria, with Cronbach's Alpha and Composite Reliability going beyond the 0.700 threshold [20], [25], [26].

D.3. Structural Model Assessment

The structural model was evaluated using the coefficient of determination (R^2), effect size (f^2), and path coefficients through a bootstrapping procedure in SmartPLS [21]. Table 5 shows that BI (R^2 = 0.700) has the largest proportion of variance. This indicates that BI has strong explanatory power, while PU and AU have moderate explanatory power.

Table 5. Coefficient Of Determination (R^2)

Endogenous Construct	R^2	Interpretation
BI	0.700	70% of BI is explained by PU, PEOU, SI, FC, and PS
PU	0.546	54.6% of PU is explained by PEOU and PS
AU	0.577	57.7% of AU is explained by BI

Next is f^2, which explains how much each exogenous construct contributes to the endogenous construct [21]. Table 6 shows the relationship between each path and its effect size.

Table 6. Effect Size (F^2)

Path	f^2
PU → BI	0.116
PEOU → BI	0.083
PEOU → PU	0.140
SI → BI	0.211
FC → BI	0.008
PS → BI	0.025
PS → PU	0.548
BI → AU	1.366

Table 6 shows that PS has a strong influence on PU (f^2 = 0.548) and BI has a significant influence on AU (f^2 = 1.366). The other relationships show small to moderate effects. This indicates that the level of influence varies between constructs.

E. Discussion

Based on the PLS-SEM analysis, six of the eight hypotheses were supported, and two were not. The six supported hypotheses were H1, H2, H3, H4, H7, and H8. Meanwhile, the two hypotheses that were not supported were H5 and H6. A summary of the analysis results is shown in Table 7.

Table 7. Hypothesis Testing Results

Hypothesis	Path Coofficient	T statistics	p-value	Decision
H1	0.323	1.802	0.072	Supported
H2	0.240	2.525	0.012	Supported
H3	0.284	3.877	0.000	Supported
H4	0.393	2.814	0.005	Supported
H5	-0.101	0.630	0.529	Not Supported
H6	0.126	0.915	0.360	Not Supported
H7	0.563	7.443	0.000	Supported
H8	0.760	14.318	0.000	Supported

Hypothesis H1 (PU → BI) suggests that perceived usefulness has a positive but weak influence on behavioral intention. This relationship is only significant at a 10% significance level, indicating that perceived usefulness is not a major factor in shaping users' intentions to use MFA in the LNSW environment. This finding differs from the research by Azhari et al [8], which states that perceived usefulness has a significant effect on the intention to use biometric security technology in the context of digital banking services in Indonesia. This is due to the difference in user context, namely banking service users compared to employees in public sector organizations.

Hypothesis H2 (PEOU → BI) shows that perceived ease of use has a positive and significant effect on behavioral intention. This finding indicates that the easier the MFA feature is to use, the higher the intention of LNSW employees to use it. These results are in line with Azhari et al [8] and Siagian et al [12], who emphasize

that ease of use is an important factor in encouraging MFA adoption, especially in organizational environments that implement mandatory usage policies.

Hypothesis H3 (PEOU → PU) shows that perceived ease of use has a positive and significant effect on perceived usefulness. This finding indicates that the easier the MFA feature is to use, the greater the perception of LNSW employees regarding the usefulness of MFA in supporting work activities. These results are in line with the findings of Azhari et al [8] and Siagian et al [12].

Hypothesis H4 (SI → BI) shows that social influence has a positive and significant effect on behavioral intention. This is in line with the research by Venkatesh et al [9] and Al-Husari et al [17] that the implementation of MFA is often driven by policy pressure within organizations. In the context of LNSW, the social environment, particularly the direction and policies of leaders, plays an important role in encouraging LNSW employees to use MFA. In public sector environments such as LNSW, decisions to implement technology tend to be influenced by organizational norms and the expectations of superiors rather than by personal desires.

Hypothesis H5 (FC → BI) shows that facilitating conditions do not have a significant effect on behavioral intention. This finding indicates that the availability of supporting facilities such as devices and infrastructure, is not a major factor in shaping LNSW employees' intention to use MFA. This result differs from the findings of Venkatesh et al [9], who stated that facilitating conditions play an important role in encouraging the intention to use technology. This difference can be explained by the context of MFA implementation at LNSW, where the authentication process can be carried out using authenticator tools and passkeys that have been installed on employees' personal devices (mobile phones). This condition makes employees consider supporting facilities as something that is already available and commonplace, so that they are no longer a consideration in forming the intention to use MFA.

Hypothesis H6 (PS → BI) shows that perceived security does not have a significant effect on behavioral intention to use MFA in the LNSW environment. This finding indicates that perceived security is not a major factor driving employees' intention to use MFA.These results differ from the findings of Azhari et al [8] and Siagian et al [12], which show that perceived security has a positive and significant effect on the intention to use digital technology, particularly in the context of financial services and digital payments, where user trust is a crucial factor in system adoption. The difference in results in the LNSW context can be explained by the characteristics of public sector organizations, where the use of MFA is mandatory and established as institutional policy. In this context, employees tend to use MFA not based on personal security perceptions, but rather because of organizational obligations. hypothesis H6 is rejected.

Hypothesis H7 (PS → PU) shows that perceived security has a positive and significant effect on perceived usefulness. This finding indicates that the higher the perception of LNSW employees regarding the security of MFA, the higher their perception of the usefulness of the system in supporting work activities. This result is in line with the findings of Azhari et al [8], which show that the perception of security in biometric authentication technology contributes to an increase in the perception of system benefits.

Hypothesis H8 (BI → AU) shows that behavioral intention has a positive and significant effect on the actual usage of MFA at LNSW. This finding indicates that the higher the intention of LNSW employees to use MFA, the more likely they are to actually use the MFA feature in their daily work activities. This finding is consistent with Davis and Azhari et al. research [7], [8], which states that behavioral intention is a direct predictor of actual system usage because it reflects an individual's readiness to act.

F. Implication and Limitation

F.1. Implication

This study offers two key implications, namely, theoretical and practical implications. The theoretical implications of this study include, first, in the context of MFA implementation in LNSW, the perceived usefulness (PU) arising from the security aspect (PS) has a greater influence than the direct influence of the security aspect on user behavioral intention (BI). Second, technology adoption theories using TAM[7] and UTAUT [9] are still very relevant, particularly the Social Influence (SI) construct, in explaining the application of MFA in the LNSW environment. Third, the TAM model, especially the Behavioral Intention construct, remains relevant for explaining technology adoption in information system security aspects, particularly in MFA implementation. The practical implication of this research is that organizations must provide a good understanding of the benefits of implementing MFA, followed by the formulation of policies related to MFA adoption.

F.2. Limitation

This study has two main limitations. First, the number of respondents is relatively limited, so the findings cannot be generalized broadly. Second, the scope of the study is limited to the internal team of LNSW and related vendors, so further research could be expanded to involve other government agencies to gain a more comprehensive understanding.

G. Conclusion

This study identifies factors that influence the adoption of Multi-Factor Authentication (MFA) by employees and vendors at LNSW. The results show that perceived ease of use (PEOU) and social influence (SI) are the main determinants of MFA usage intention, while perceived security (PS) plays an indirect role through increased perceived usefulness (PU). In addition, intention to use (BI) was found to be the main predictor of actual use (AU) of MFA.

These findings confirm that the TAM and UTAUT models are still relevant in explaining the adoption of security technology in the public sector, particularly in the context of MFA. Based on these results, LNSW is advised to improve employees' understanding of the importance of implementing MFA, especially by emphasizing the benefits gained in supporting work activities and system protection. This study has limitations in terms of the number of respondents and the scope of the organization, so further research is recommended to involve more stakeholders across agencies to improve the generalization of the findings

H. Acknowledgment

The authors would like to express their sincere gratitude to the Indonesia National Single Window Agency (LNSW) for providing the necessary data and supporting this research. The authors also extend their appreciation to Universitas of Indonesia for facilitating and supporting the implementation of this study.

I. References

[1] UNECE, Recommendation and Guidelines on establishing a Single Window to enhance the efficient exchange of information between trade and government : recommendation no. 33. UN, 2005.

[2] UNECE, "Information Service United Nations Economic Commission for Europe 2020 Edition," 2020. [Online]. Available: http://www.unece.org

[3] J. Van Der Ham, "Toward a Better Understanding of 'Cybersecurity,'" Digital Threats: Research and Practice, vol. 2, no. 3, Jun. 2021, doi: 10.1145/3442445.

[4] B. Lundgren and N. Möller, "Defining Information Security," Sci. Eng. Ethics, vol. 25, no. 2, pp. 419–441, Apr. 2019, doi: 10.1007/s11948-017-9992-1.

[5] C. Kar Yee and M. F. Zolkipli, "Review on Confidentiality, Integrity and Availability in Information Security," Journal of ICT in Education, vol. 8, no. 2, pp. 34–42, Jul. 2021, doi: 10.37134/jictie.vol8.2.4.2021.

[6] "Lanskap Keamanan Siber Indonesia 2024," 2024.

[7] F. D. Davis, "Perceived Usefulness, Perceived Ease Of Use, And User Accep Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology."

[8] S. C. Azhari, A. Permatasari, and M. Angelus, "Implementation of Biometric Technology in Indonesian Mobile Banking: A TAM Perspective on Enhancing Transaction Security and Enjoyment," in Proceedings of 8th International Conference on Inventive Computation Technologies, ICICT 2025, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 152–158. doi: 10.1109/ICICT64420.2025.11005053.

[9] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Q., vol. 27, no. 3, pp. 425–478, 2003, doi: 10.2307/30036540.

[10] Z. Kenesei, L. Kökény, K. Ásványi, and M. Jászberényi, "The central role of trust and perceived risk in the acceptance of autonomous vehicles in an integrated UTAUT model," European Transport Research Review, vol. 17, no. 1, Dec. 2025, doi: 10.1186/s12544-024-00681-x.

[11] M. C. Libicki, E. Balkovich, B. A. Jackson, R. Rudavsky, and K. Watkins Webb, "HOMELAND SECURITY AND DEFENSE CENTER For More Information." [Online]. Available: www.rand.org

[12] H. Siagian, Z. J. H. Tarigan, S. R. Basana, and R. Basuki, "The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform," International Journal of Data and Network Science, vol. 6, no. 3, pp. 861–874, Jun. 2022, doi: 10.5267/j.ijdns.2022.2.010.

[13] J. Jiaxin Zhang, Y. Luximon, and Y. Song, "The role of consumers' perceived security, perceived control, interface design features, and conscientiousness

in continuous use of mobile payment services," Sustainability (Switzerland), vol. 11, no. 23, Dec. 2019, doi: 10.3390/su11236843.

[14] P. T. Tran-Truong et al., "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis," May 01, 2025, Elsevier B.V. doi: 10.1016/j.sysarc.2025.103402.

[15] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," Comput. Secur., vol. 95, Aug. 2020, doi: 10.1016/j.cose.2020.101745.

[16] A. Nanda, J. J. Jeong, S. W. A. Shah, M. Nosouhi, and R. Doss, "Examining usable security features and user perceptions of Physical Authentication Devices," Comput. Secur., vol. 139, Apr. 2024, doi: 10.1016/j.cose.2023.103664.

[17] F. Al-Husari, O. Nakov, and P. Nakov, "Multi-Factor Authentication Fatigue: A Growing Concern in User Experience and Security," in 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies, ICEST 2025 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2025. doi: 10.1109/ICEST66328.2025.11098219.

[18] M.-M. D'costa-Alphonso and M. Lane, "The Adoption of Single Sign-On and Multifactor Authentication in Organisations: A Critical Evaluation Using TOE Framework," Issues in Informing Science and Information Technology, vol. 7, pp. 161–189, 2010, doi: 10.28945/1199.

[19] J. J. Jeong, S. W. A. Shah, A. Nanda, R. Doss, M. Nosouhi, and J. Webb, "User Characteristics and Their Impact on the Perceived Usable Security of Physical Authentication Devices," IEEE Trans. Hum. Mach. Syst., vol. 54, no. 5, pp. 554–564, 2024, doi: 10.1109/THMS.2024.3421538.

[20] O. J. Aburumman, K. Omar, M. Al Shbail, and M. Aldoghan, "How to Deal with the Results of PLS-SEM?," in Lecture Notes in Networks and Systems, Springer Science and Business Media Deutschland GmbH, 2023, pp. 1196–1206. doi: 10.1007/978-3-031-08954-1_101.

[21] V. Genia, I. Eitiveni, M. R. Tirtayasa, W. S. Wibowo, T. F. Nugraha, and T. Nabarian, "Unraveling The Key Factors Of Successful Erp Post Implementation In The Indonesian Construction Context," Interdisciplinary Journal of Information, Knowledge, and Management, vol. 18, pp. 513–545, 2023, doi: 10.28945/5177.

[22] M. R. Ab Hamid, W. Sami, and M. H. Mohmad Sidek, "Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion," in Journal of Physics: Conference Series, Institute of Physics Publishing, Sep. 2017. doi: 10.1088/1742-6596/890/1/012163.

[23] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," Jan. 14, 2019, Emerald Group Publishing Ltd. doi: 10.1108/EBR-11-2018-0203.

[24] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, and K. O. Thiele, "Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods," J. Acad. Mark. Sci., vol. 45, no. 5, pp. 616–632, Sep. 2017, doi: 10.1007/s11747-017-0517-x.

[25] S. M. Rasoolimanesh, "Discriminant validity assessment in PLS-SEM: A comprehensive composite-based approach," 2022. [Online]. Available: https://www.scriptwarp.com,

[26] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," J. Acad. Mark. Sci., vol. 43, no. 1, pp. 115–135, Jan. 2015, doi: 10.1007/s11747-014-0403-8.