Digital Identity and Information Security: A Behavioral Approach

Nguyen Thi Hoi
Faculty of Economic Information System and E-commerce, Thuongmai University, Vietnam
&
Dam Gia Manh
Department of Information Technology, Dong Do Unuversity, Vietnam

DOI: https://doi.org/10.56293/IJMSSSR.2026.6205

IJMSSSR 2026
VOLUME 8
ISSUE 3 MAY - JUNE **ISSN: 2582 – 0265**

Abstract: In the context of accelerating digital transformation, digital identity has become a critical component of cybersecurity, enabling the protection of personal data and secure access in cyberspace. The rapid expansion of digital platforms has intensified cyber threats, including identity fraud, data breaches, and unauthorized access. Effective digital identity management is therefore essential for ensuring authentication, access control, and compliance with regulatory frameworks such as the GDPR and the CCPA. This study examines the structure and vulnerabilities of digital identities and evaluates existing security mechanisms, including multi-factor authentication (MFA), privileged access management, and real-time identity verification. Drawing on a behavioral and governance-oriented perspective, the research proposes integrated technical and policy-driven solutions to enhance personal information security. The findings highlight the importance of combining identity governance with user-centric security practices to mitigate risks associated with digital identity compromise. This study contributes to the literature by providing a comprehensive framework for strengthening digital identity security in increasingly complex digital ecosystems.

Keywords: Digital identity; Personal data protection; Cyberspace security; TAM; TPB.

1. INTRODUCTION

In the era of rapid digital transformation, cyberspace has evolved into a complex and interconnected environment that integrates telecommunication networks, cloud computing systems, and digital infrastructures, enabling seamless communication, economic exchange, and knowledge dissemination (Floridi, 2015). This digital ecosystem not only enhances socio-economic development but also plays a critical role in governance, cultural exchange, and national security. Within this context, digital identity has emerged as a fundamental mechanism for representing and authenticating individuals and entities in online environments.

Digital identity, defined as a structured set of personal data used for identification in digital interactions, is essential for enabling secure access, validating transactions, and protecting user privacy (Ometov et al., 2018). Beyond its functional role, digital identity contributes to enhancing personalization, user experience, and compliance with regulatory frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). However, as digital services continue to expand, the increasing reliance on digital identities has also amplified exposure to cybersecurity threats.

Cyberspace remains vulnerable to various forms of cyberattacks, including phishing, identity theft, malware infiltration, and unauthorized system access. To address these risks, organizations have implemented advanced security mechanisms such as multi-factor authentication (MFA), encryption protocols, and access control systems (Sergey et al., 2018). Despite these efforts, cybercriminals increasingly exploit digital identities as entry points for system intrusion and data breaches. Recent reports indicate that 26% of security incidents in 2023 were associated with the misuse of valid credentials (Magrane, 2023), while authentication activities have surged significantly, with over 16 billion authentication requests recorded globally (Halpin, 2024). These trends highlight the urgent need

for more robust and user-centric identity protection frameworks.

In the Vietnamese context, cybersecurity challenges are becoming increasingly severe. According to the Department of Cybersecurity and High-Tech Crime Prevention (Ministry of Public Security, 2022), millions of cyberattack alerts were recorded within a short period, including targeted attacks on government systems and widespread malware infections. These statistics underscore the necessity of strengthening digital identity protection at both individual and institutional levels.

From a behavioral perspective, understanding how users perceive and adopt digital identity systems is essential for enhancing security outcomes. This study integrates established behavioral theories, including the TPB (Ajzen, 1991) and the TAM (Davis, 1989), to examine the determinants of digital identity adoption. Additionally, the TRA (Ajzen & Fishbein, 1975) and trust-based frameworks (Gefen et al., 2003) are incorporated to provide a comprehensive explanation of user intentions and security-related behaviors.

Building on recent empirical research, prior studies have highlighted the role of advanced authentication technologies in reducing data leakage (Tuan et al., 2022) and the rapid growth of digital financial services in Vietnam (Trang & Minh, 2023). Moreover, emerging research emphasizes the importance of user profiling and behavioral analytics in strengthening cybersecurity systems (Foroughi & Luksch, 2018; Puricato et al., 2024). However, a critical gap remains in integrating behavioral insights with digital identity governance to enhance personal information security.

Therefore, this study aims to develop an integrated framework that combines behavioral models and cybersecurity mechanisms to explain digital identity construction and its impact on personal information protection. By bridging the gap between user behavior and identity governance, the research contributes to the development of more secure, resilient, and user-centric digital ecosystems.

2. THE RESEACH MODEL

2.1. Environmental factors

Environmental factors play a critical role in shaping users' behavioral intentions to construct and maintain digital identities in cyberspace. Among these, governmental policies and technological infrastructure are key determinants influencing user engagement in digital identity ecosystems. Favorable regulatory frameworks, particularly those related to online registration and data governance, enhance user participation by ensuring transparency, privacy protection, and data ownership rights (Voigt & von dem Bussche, 2021). When users perceive that their personal information is adequately protected, they are more likely to adopt secure digital identity practices. This perspective aligns with the TRA, which emphasizes the role of external conditions in shaping attitudes and behavioral intentions (Ajzen & Fishbein, 1980).

H1: Government policies on privacy and personal data protection positively influence users' intention to construct digital identities.

Technological infrastructure also plays a crucial role in enabling secure identity adoption. High-quality digital systems, supported by advanced security features such as multi-factor authentication, biometric verification, and encryption, enhance both accessibility and trust (Ometov et al., 2022). According to the TAM, perceived usefulness and ease of use significantly influence user adoption (Davis, 1989; Venkatesh & Davis, 2000).

H2: Technological infrastructure positively influences users' intention to construct and maintain digital identities.

2.2. Organizational factors

Organizational readiness and strategic involvement in digital transformation significantly influence users' behavioral intentions toward digital identity adoption. Organizational digital readiness not only improves internal efficiency but also strengthens the broader digital ecosystem (Hoang Ha, 2023). In this context, organizations act

as key enablers by implementing supportive policies, secure infrastructure, and transparent data practices.

According to the organizational trust model, competence, integrity, and benevolence are essential in building user trust (Mayer, Davis, & Schoorman, 1995). In digital identity systems, trust plays a critical role in encouraging user participation and sustained engagement. Additionally, organizations with strong innovation capabilities are more likely to develop user-centric and scalable identity solutions. The integration of advanced technologies such as AI-based authentication, intuitive interfaces, and consistent service quality enhances user experience and reinforces adoption (Puricato et al., 2024).

H3: Organizational factors positively influence users' behavioral intention to construct digital identities.

2.3. Personal factors

Personal factors play a crucial role in shaping users' behavioral intentions toward digital identity construction. Prior research highlights that individual attitudes toward technology significantly influence adoption behavior (Chan & Lu, 2004). Grounded in the TRA, attitudes are key determinants of behavioral intention (Ajzen, 1991). When users perceive clear benefits of digital identity, such as convenience, enhanced security, and better control over personal data, they are more likely to develop positive attitudes and engage in identity construction.

In addition, personal confidence in the reliability and security of digital identity systems further strengthens behavioral intention. Users who trust that their data is protected are more willing to adopt and continuously use digital identity services. Therefore, both positive attitudes and confidence act as critical drivers of user participation in digital identity ecosystems.

H4: Personal factors positively influence users' behavioral intention to construct digital identities.

2.4. Digital identity usage behavior

Digital identity usage behavior is a multidimensional construct shaped by technological readiness, psychological factors, and environmental conditions, reflecting how individuals interact with digital identity systems across platforms and over time (Kirkpatrick et al., 2022). This behavior is increasingly associated with broader societal objectives, including cybersecurity resilience, transactional accountability, and digital empowerment (Ometov et al., 2022; World Bank, 2023).

The TAM provides a foundational explanation, suggesting that perceived usefulness and ease of use are key drivers of adoption (Davis, 1989). In the context of digital identity, system usability, interoperability, and real-time responsiveness significantly enhance user engagement (Venkatesh & Davis, 2000; Al-Qaysi et al., 2023). In addition, trust is a central determinant, as users are more likely to adopt platforms perceived as secure, transparent, and reliable (Camp, 2001; Ometov et al., 2022). Emerging technologies such as blockchain-based identity systems and zero-trust architectures further reinforce system credibility and user confidence (Halpin, 2024; Zhang et al., 2024).

Behavioral theories, including the TRA and the TPB, emphasize that attitudes, subjective norms, and perceived behavioral control shape user intentions (Ajzen, 1991). Complementary frameworks such as MOA and UTAUT highlight the roles of motivation, ability, and facilitating conditions in translating intention into actual behavior (Venkatesh et al., 2003; Puricato et al., 2024).

H5: Behavioral intention to use digital identity positively influences intention to construct digital identities.
H6: Trust in digital identity positively influences intention to construct digital identities.
H7: Digital identity usage behavior positively influences intention to construct digital identities.

2.5. Proposed research model

The proposed research model examines the multidimensional determinants influencing individuals' behavioral intention and actual decision to construct digital identities. Grounded in the TAM, the TPB, and the UTAUT, the model integrates both behavioral and institutional perspectives to provide a comprehensive analytical framework. In the context of rapid digital transformation, digital identity has become a critical mechanism for enabling secure access to services, facilitating digital transactions, and protecting personal data. However, the decision to construct and maintain digital identities remains a complex process shaped by interrelated factors, including regulatory environments, technological capabilities, organizational support, and individual perceptions.

The proposed model incorporates seven hypotheses (H1–H7), capturing macro-, meso-, and micro-level determinants. These include government policies on privacy and data protection, technological infrastructure, organizational factors, and personal factors, as well as behavioral intention, trust in digital identity systems, and prior usage behavior. These constructs are hypothesized to influence users' intention to construct digital identities, which subsequently drives their actual adoption decisions.

Details of the proposed research model are summarized in Table 1

Table 1: Table of factors proposed in the model

Hypothesis	Factors	Contents	Reference model
H1 (MTN)	MTN1	Government regulations on digital identity influence my decision to adopt it.	World Bank, 2023; OECD, 2023
	MTN2	Security policies on digital identity enhance my intention to develop a digital identity.	Halpin, 2024; European Commission, 2022
	MTN3	Legal frameworks and data protection policies support my willingness to establish a digital identity.	OECD, 2023; Ometov et al., 2022
	MTN4	There is a need for additional government policies to ensure digital identity protection.	UNDP, 2023; Halpin, 2024
	MTN5	Personal data protection laws raise my awareness of digital identity safety.	European Commission, 2022; World Bank, 2023
H2 (MTC)	MTC1	Emerging technologies drive my need to establish a digital identity.	Zhang, Yang, & Wang, 2024; OECD, 2023
	MTC2	The growth of electronic transaction services increases my demand for a secure digital identity.	World Bank, 2023; UNDP, 2023
	MTC3	I receive adequate information and guidance about security risks related to digital identity.	Ometov et al., 2022; European Commission, 2022
	MTC4	The registration and authentication process for digital identity is user-friendly and easy to use.	Alalwan et al., 2021; Venkatesh & Davis, 2000
H3 (TC)	TC1	My organization's structure requires me to create a digital identity.	UNDP, 2023; Alalwan et al., 2021
	TC2	Digital systems, legal policies, and data protection practices influence my organization's digital identity requirements.	OECD, 2023; European Commission, 2022
	TC3	The requirement for maintaining digital records encourages me to establish a digital identity.	World Bank, 2023; Ometov et al., 2022
	TC4	I must establish a digital identity to access internal organizational systems or services.	Venkatesh et al., 2003; Magrane, 2023
	TC5	My confidence in building a secure digital identity increases when my organization uses advanced security technologies.	Camp, 2001; Zhang, Yang, & Wang, 2024
H4 (CN)	CN1	I understand the importance of digital identity in digital	Kotler & Keller, 2022;

		society.	Ajzen, 1991
	CN2	I am aware that digital identity authentication helps protect my personal information.	Camp, 2001; Ometov et al., 2022
	CN3	I need digital identity systems to secure my personal and banking information.	Zhang, Yang, & Wang, 2024; European Commission, 2022
	CN4	My workplace or university requires me to digitalize my personal data.	UNDP, 2023; Venkatesh et al., 2003
	CN5	I am willing to use digital identity for digital services if security is guaranteed.	Alalwan et al., 2021; Halpin, 2024
	CN6	I know that a reliable digital identity improves my access to online services.	World Bank, 2023; OECD, 2023
H5 (HVY)	HVY1	My decision to establish a digital identity is influenced by family and friends.	Venkatesh et al., 2003; Bente, 2024
	HVY2	Media and online information shape my intention to adopt digital identity.	Fishbein & Ajzen, 1975; OECD, 2023
	HVY3	I frequently use digital identity for payments, shopping, or public services.	Ometov et al., 2022; World Bank, 2023
	HVY4	I distinguish between the importance of accounts to apply suitable security.	Zhang, Yang, & Wang, 2024; Camp, 2001
	HVY5	I have secure and reliable experiences when using digital identity for login.	Halpin, 2024; Alalwan et al., 2021
H6 (HVM)	HVM1	I feel secure sharing personal information with reputable organizations to build a digital identity.	Camp, 2001; Ometov et al., 2022
	HVM2	I am willing to establish a digital identity when security systems are adequately ensured.	Halpin, 2024; Zhang, Yang, & Wang, 2024
	HVM3	I hesitate to build a digital identity when I feel my privacy is at risk.	European Commission, 2022; OECD, 2023
	HVM4	I trust digital identity platforms more when organizations show respect for user privacy.	UNDP, 2023; World Bank, 2023
	HVM5	I feel comfortable sharing personal contact information with digital service platforms.	Alalwan et al., 2021; Kotler & Keller, 2022
	HVM6	I actively seek out and update my knowledge about digital identity security.	Ometov et al., 2022; Zhang et al., 2024
H7 (HV)	HV1	Awareness of the benefits of digital identity strengthens my intention to establish one.	Kotler & Keller, 2022; Venkatesh & Davis, 2000
	HV2	Awareness of digital identity risks motivates me to manage and establish my identity securely.	Ometov et al., 2022; European Commission, 2022
	HV3	Trust in digital identity systems increases my intention to adopt them.	Camp, 2001; Halpin, 2024
	HV4	I feel in control of the process, which enhances my willingness to establish a digital identity.	Ajzen, 1991; Venkatesh et al., 2003
	HV5	The perceived cost of using digital identity reduces my intention to establish one.	Fishbein & Ajzen, 1975; OECD, 2023
QD	QD1	I am likely to recommend digital identity services to others soon.	Venkatesh et al., 2003; Kotler & Keller, 2022
	QD2	I intend to increase my usage of digital identity services in the near future.	Venkatesh & Davis, 2000; Alalwan et al., 2021
	QD3	I will stay informed to protect my digital identity.	Ometov et al., 2022;

			Halpin, 2024
	QD4	I choose to use digital identity when engaging in online activities.	World Bank, 2023; OECD, 2023

3. METHODOLOGY

This study provides a comprehensive examination of the factors influencing digital identity construction in cyberspace, focusing on behavioral, technological, organizational, and policy determinants. Grounded in digital transformation and cybersecurity perspectives, the research adopts a quantitative approach to ensure objective and measurable insights (Creswell & Creswell, 2018; Saunders et al., 2019).

Using validated scales from prior studies, key constructs were measured on a five-point Likert scale (Kim & Forsythe, 2021; Ometov et al., 2022). The quantitative design enables the empirical testing of relationships between variables such as trust, digital literacy, and legal environment, and outcomes including behavioral intention and actual adoption (Hair et al., 2022).

Data were analyzed using SPSS and AMOS, following a structured process: Descriptive Statistics, Cronbach's Alpha, EFA, CFA, and SEM. This approach ensures reliability, validity, and model fit, supporting robust evaluation of the proposed research model.

4. RESULTS AND DISCUSSION

4.1. Descriptive statistics

The descriptive analysis of 250 respondents indicates a relatively balanced gender distribution, with females accounting for 54.6% (n = 136) and males 45.4% (n = 114). The sample is predominantly composed of university students (60.4%, n = 151), followed by individuals with less than five years of work experience (18.4%, n = 46), reflecting a young and digitally active population.

Regarding attitudes toward digital identity construction, 36.4% of respondents expressed concern (n = 91), while 16.4% demonstrated strong concern and willingness to adopt (n = 41). A notable proportion remained neutral (29.2%, n = 73), with smaller shares slightly concerned (14%, n = 35) or not concerned (4%, n = 10). Overall, the findings suggest a generally positive yet cautious attitude toward digital identity adoption.

4.2. Cronbach's Alpha test

The reliability of measurement scales was assessed using Cronbach's Alpha, a widely accepted indicator of internal consistency. As shown in Table 3, all constructs achieved alpha values above the minimum threshold of 0.600, acceptable for exploratory research (Hair et al., 2022). Specifically, coefficients ranged from 0.681 to 0.901, indicating moderate to high reliability (George & Mallery, 2019).

According to Nunnally and Bernstein (1994), values above 0.7 are considered satisfactory for confirmatory studies, while levels above 0.6 remain acceptable in early-stage research.

Additionally, item-total correlation coefficients for all variables exceeded 0.30, meeting the recommended threshold for meaningful contribution to the scale (DeVellis, 2017). These findings are consistent with recent measurement theory emphasizing the importance of internal consistency and unidimensionality (Joe et al., 2023).

Table 2: Summary of Cronbach's Alpha scale

Hypothesis	Symbol	Initial variable	Remaining variable	Cronbach's Alpha	Number of variables excluded
H1	MTN	5	4	0.674	1

H2	MTC	5	5	0.734	0
H3	TC	5	5	0.851	0
H4	CN	6	5	0.829	0
H5	HVY	5	5	0.801	0
H6	HVM	6	6	0.815	0
H7	HV	5	5	0.779	0
	QD	4	4	0.801	0
Total		41	40		1

(Source: Results of survey questionnaire analysis using SPSS)

Overall, the results confirm that the measurement scales are reliable and suitable for subsequent EFA.

4.3. EFA ressult

The Exploratory Factor Analysis (EFA) results indicate that 31 observed variables were grouped into six latent factors. The Kaiser-Meyer-Olkin (KMO) value of 0.780 confirms sampling adequacy, exceeding the acceptable threshold (Hair et al., 2019). Bartlett's Test of Sphericity is significant ($\chi^2 = 2576.779$, $p < .001$), indicating sufficient correlations among variables for factor analysis (Field, 2018). These results confirm that the dataset meets the necessary conditions for EFA.

Furthermore, the six extracted factors explain 57.135% of the total variance, exceeding the recommended threshold of 50% (Williams et al., 2010). This level of explained variance suggests that the factor structure adequately represents the underlying data. According to psychometric standards, such results provide strong support for construct validity and dimensionality (Costello & Osborne, 2005; Howard, 2016).

Overall, the EFA findings confirm that the measurement model is both statistically robust and conceptually valid.

4.4. SEM Analysis

Structural Equation Modeling (SEM) was employed to validate the hypothesized relationships among latent constructs, enabling simultaneous assessment of both measurement and structural models (Hair et al., 2019). The SEM results, presented in Table 3, include standardized and unstandardized path coefficients, critical ratios (C.R.), and p-values to evaluate the strength and significance of each relationship.

Prior to SEM, Confirmatory Factor Analysis (CFA) confirmed an acceptable model fit. The chi-square test indicated adequacy ($p > .05$), while TLI and CFI values exceeded 0.90, demonstrating strong comparative fit (Hu & Bentler, 1999; Tucker & Lewis, 1973). Additionally, the normed chi-square (CMIN/df = 1.360) and RMSEA (0.038) fall well within recommended thresholds, confirming excellent model fit (Hair et al., 2019; Schreiber et al., 2006).

Measurement validity and reliability were further supported by CR, AVE, and convergent validity. All factor loadings exceeded 0.50, with many above 0.70, indicating strong construct representation (Fornell & Larcker, 1981). Overall, the results confirm the robustness of the model and the validity of the hypothesized relationships.

Table 3: Regression Coefficients of the Final Research Model

Relationship	Unstandardized Coefficient	Standardized Coefficient	Standard Error (S.E)	Critical Ratio (C.R)	P-value (P)	Accepted/ Excluded
HV ← TC	.183	0.179	.091	2.025	.043	Accepted

HV ← HVY	.204	0.265	.071	2.881	.004	Accepted
HV ← MTN	.027	.025	.087	.305	.760	Excluded
QD← TC	.032	.028	.102	.319	.750	Excluded
QD ← HVY	.033	.037	.080	.408	.683	Excluded
QD ← MTN	.422	.343	.106	4.002	***	Accepted
QD ← HV	.256	.225	.096	2.667	.008	Accepted

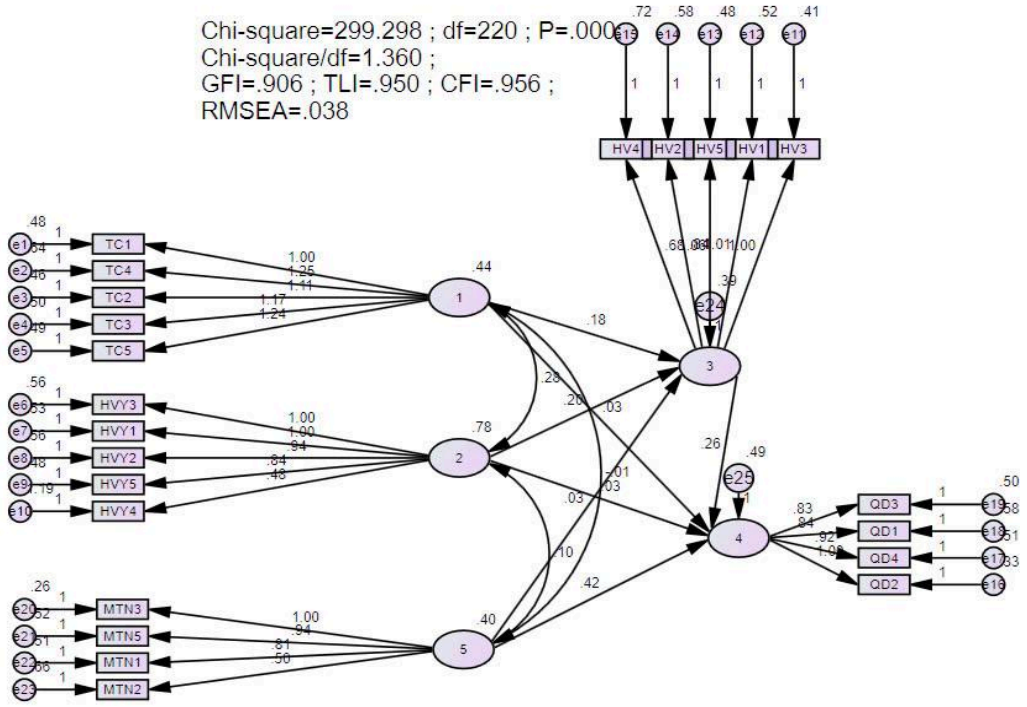

Figure 1: SEM Result

(Source: Results of survey analysis using AMOS)

The SEM results provide important insights into the relationships among key constructs. Technological Confidence (TC) and Perceived Behavioral Control (HVY) have significant positive effects on Behavioral Intention (HV), with standardized coefficients of 0.265 and 0.179 ($p < .001$), highlighting the role of user confidence and perceived control in digital identity adoption (Venkatesh et al., 2012).

Additionally, Motivation (MTN) and Behavioral Intention (HV) significantly influence Quality of Decision (QD), with coefficients of 0.422 and 0.256, respectively. These findings align with TRA and TAM, emphasizing the importance of motivation and intention in shaping decision outcomes (Ajzen & Fishbein, 1980; Davis, 1989).

Conversely, the relationships between TC–QD, HVY–QD, and MTN–HV are not statistically robust, suggesting limited predictive strength (Kline, 2015). Overall, the findings highlight the importance of confidence, control, motivation, and intention in enhancing digital identity adoption and decision quality, offering valuable implications for developing secure and user-centric digital identity systems (Bélanger & Crossler, 2011; Pavlou, 2011).

4.5. Discussion of results

The empirical results obtained from SPSS and AMOS analyses provide strong support for the proposed structural model, demonstrating satisfactory model fit and explanatory power. SEM findings confirm that hypotheses H1, H3, H5, and H7 are statistically significant ($p < 0.05$; C.R. > 1.96). Specifically, government policies on privacy and data protection (H1) and digital identity usage behavior (H7) play critical roles in shaping users' intention to construct digital identities. In addition, organizational factors (H3) and behavioral intention (H5) significantly enhance trust, which is essential for secure digital identity adoption (Venkatesh et al., 2012; Bélanger & Crossler, 2011).

These findings are consistent with prior studies highlighting the importance of regulatory frameworks and organizational readiness in technology adoption. In contrast, hypotheses H2, H4, and H6 are not statistically significant, suggesting that technological infrastructure, personal factors, and trust do not exert direct effects. This may reflect limited user awareness and varying levels of technological readiness, particularly in emerging contexts (Rogers, 2003; Dwivedi et al., 2021).

Reliability and validity are confirmed through EFA and CFA, with strong internal consistency and construct validity (Hair et al., 2019; Fornell & Larcker, 1981). Overall, the model emphasizes the importance of policy, organizational readiness, and user behavior in promoting digital identity adoption.

5. IMPLICATIONS AND CONCLUSION

Based on the empirical findings, this study provides several important insights into the factors influencing digital identity construction in a rapidly evolving digital environment. First, the Government Environment plays a significant role in shaping users' decisions, as regulatory clarity, data protection policies, and investment in digital infrastructure enhance trust and encourage adoption. In contexts with strong legal frameworks, individuals demonstrate greater confidence and willingness to transition to digital identity systems, whereas uncertainty and privacy concerns may hinder adoption (Bélanger & Crossler, 2011; Pavlou, 2011; Dwivedi et al., 2021).

Second, Organizational Factors and Prior Usage Behavior significantly influence user Behavior toward digital identity construction. Supportive organizational policies, effective onboarding processes, and technological standards reduce perceived risk and foster engagement. Additionally, individuals with prior digital experience are more likely to adopt and sustain digital identity usage (Ajzen & Fishbein, 1980; Lim et al., 2022).

Third, user Behavior directly impacts Decision-making, indicating that habitual engagement and digital literacy are critical drivers of adoption (Gefen et al., 2003). However, some relationships show limited practical significance, suggesting that final decisions are shaped by a complex interaction of trust, perceived value, and risk assessment rather than single factors (Kim et al., 2009; McKnight et al., 2011).

From a practical perspective, governments should strengthen legal frameworks and promote public awareness, while organizations should adopt user-centric strategies, including training and transparent communication. Individuals must enhance digital literacy to effectively engage with identity systems. Future research should explore moderating factors such as trust, risk perception, and technological readiness across different user segments.

Overall, this study contributes a comprehensive framework integrating behavioral and institutional perspectives, offering valuable implications for developing secure, inclusive, and sustainable digital identity ecosystems.

References

1. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
2. Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2021). Digital identity systems: Adoption factors and behavioural outcomes. Information Systems Frontiers, 23(1), 101–121.
3. Alashoor, T., Han, S., & Joseph, R. C. (2021). Towards digital identity: The role of government regulation and user trust. Information Systems Frontiers, 23(3), 643–658. https://doi.org/10.1007/s10796-019-09949-z

4. Camp, L. J. (2001). Trust and risk in Internet commerce. MIT Press.
5. Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. Practical Assessment, Research & Evaluation, 10(7), 1–9.
6. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.
7. Chou, C. P., & Bentler, P. M. (1995). Estimates and tests in structural equation modeling. In R. H. Hoyle (Ed.), Structural equation modeling: Concepts, issues, and applications (pp. 37–55). Sage Publications.
8. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
9. DeVellis, R. F. (2017). Scale development: Theory and applications (4th ed.). SAGE Publications.
10. Dwivedi, Y. K., Shareef, M. A., Simintiras, A. C., Weerakkody, V., & Kumar, V. (2021). A generalised adoption model for services: A cross-country comparison of mobile health (m-health). Government Information Quarterly, 38(1), 101533. https://doi.org/10.1016/j.giq.2020.101533
11. European Commission. (2022). Data protection rules as a trust-enabler in the EU and beyond – Taking stock.
12. Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). Sage Publications.
13. Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Addison-Wesley.
14. Foroughi, F., & Luksch, P. (2018). Observation measures to profile user security behaviour. In Proceedings of the 2018 Cyber Security in Networking Conference (pp. 1–6). IEEE.
15. Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). Sage Publications.
16. Halpin, H. (2024). Decentralized identity and trust frameworks in the post-platform internet. Computer Law & Security Review, 50, 105859.
17. Hoang, H. (2023). Organizational digital readiness and citizen engagement in Vietnam's digital era. Vietnam Journal of Digital Transformation, 1(1), 25–39.
18. Howard, M. C. (2016). A review of exploratory factor analysis decisions and overview of current practices: What we are doing and how can we improve? International Journal of Human-Computer Interaction, 32(1), 51–62. https://doi.org/10.1080/10447318.2015.1087664
19. Kim, J., & Forsythe, S. (2021). The effects of sensory enabling technology on consumers' product attitudes and purchase intentions in an online store. Journal of Retailing and Consumer Services, 58, 102280. https://doi.org/10.1016/j.jretconser.2020.102280
20. Kline, R. B. (2015). Principles and practice of structural equation modeling (4th ed.). Guilford Press.
21. Kotler, P., & Keller, K. L. (2022). Marketing management (16th ed.). Pearson.
22. Magrane, B. (2023). Credential theft and misuse: Analyzing global trends in identity-based attacks. Cybersecurity Insights.
23. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.
24. OECD. (2023). Digital identity and data governance: Shaping policies for trust and inclusion. OECD Publishing.
25. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). A survey on digital identity management systems. Computer Networks, 146, 112–131. https://doi.org/10.1016/j.comnet.2018.09.002
26. Puricato, E., Boratto, L., & De Luca, E. W. (2024). User modeling and user profiling: A comprehensive survey. Journal of Web Intelligence, 22(1), 1–25. https://doi.org/10.1016/j.webint.2024.101123
27. Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson Education.
28. Tero, T., Kalakota, R., & Robinson, M. (2004). The digital identity ecosystem. Journal of Electronic Commerce Research, 5(4), 220–233.
29. Trang, A. Q., & Minh, C. H. (2023). Tác động của hành vi đánh cắp danh tính trực tuyến đến ý định sử dụng dịch vụ ngân hàng điện tử tại Việt Nam trong bối cảnh bất định. Tạp chí Kinh tế và Phát triển, 302(4), 55–66.
30. UNDP. (2023). Digital identity and inclusive development: A policy framework for sustainable transformation.

31. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model. Management Science, 46(2), 186–204.
32. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178. https://doi.org/10.2307/41410412
33. Vietnam Ministry of Public Security. (2022). Báo cáo an ninh mạng và phòng chống tội phạm công nghệ cao 2022. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao
34. Voigt, P., & von dem Bussche, A. (2021). The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing.
35. Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Review Press.
36. World Bank. (2023). Digital ID for development: Global progress and policy outlook. https://www.worldbank.org/digitalid
37. Zhang, Y., Yang, G., & Wang, H. (2024). Blockchain-enabled digital identity for privacy-preserving systems. IEEE Internet of Things Journal, 11(1), 89–103.