International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, page no. 49-74

To cite this article: Nguyen Thi Hoi (2025). FACTORS INFLUENCING DIGITAL IDENTITY FORMATION: EVIDENCE FROM HANOI, International Journal of Education and Social Science Research (IJESSR) 8 (5): 49-74 Article No. 1134, Sub Id 1766

FACTORS INFLUENCING DIGITAL IDENTITY FORMATION: EVIDENCE FROM HANOI

Nguyen Thi Hoi

Thuongmai University, Faculty of Economic Information System and E-commerce,
79 Ho Tung Mau Street, Cau Giay District, Hanoi, Vietnam

DOI : https://doi.org/10.37500/IJESSR.2025.8504

ABSTRACT

In the context of accelerating digital transformation, digital identity has become a cornerstone of cybersecurity, playing a crucial role in safeguarding personal data and ensuring secure access mechanisms in cyberspace. The proliferation of digital services and online platforms has heightened cyber threats, with rising incidents of identity fraud, data breaches, and unauthorized intrusions. Consequently, robust digital identity management is essential, not only for authentication and access control but also for compliance with international regulatory frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). However, the compromise of digital identities poses severe risks, enabling malicious actors to infiltrate sensitive systems and exploit personal information. In response, technologies such as multi-factor authentication (MFA), privileged access management, and real-time identity verification have become increasingly important for strengthening security resilience. This study examines the factors influencing users' decisions in constructing their digital identities, offering recommendations to enhance identity governance and cybersecurity, and contributing to the development of a sustainable framework for digital identity protection in the era of hyperconnectivity.

KEYWORDS: Digital identity, Cyberspace, information security, TBP, TAM

1. INTRODUCTION

In the era of rapid digitalization, cyberspace is conceptualized as a complex, interconnected environment encompassing information technology systems, including telecommunication networks, the Internet, computer infrastructure, and cloud-based databases. This digital ecosystem enables individuals and organizations to transcend physical and temporal boundaries, thereby facilitating real-time social interaction, commercial exchange, knowledge dissemination, and public governance (Floridi, 2015). Cyberspace plays an increasingly critical role in national sovereignty protection, socio-economic development, and cultural communication, underpinning the foundations of the digital society. Within this environment, digital identity serves as the core mechanism for authenticating and managing users' presence in online activities. Defined as a structured collection of personal information used to identify individuals or entities in digital contexts, digital identity is fundamental for ensuring secure access, validating transactions, protecting privacy, and mitigating fraudulent behaviors on digital platforms (Ometov et al., 2018). Beyond enhancing user experience, digital identities are instrumental in promoting security, personalization, and compliance with legal frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Despite its transformative potential, cyberspace remains vulnerable to a wide array of cybersecurity threats, including phishing attacks, identity theft, malware infiltration, and unauthorized system access. In response, cybersecurity protocols such as multi-factor authentication (MFA) (Sergey et al., 2018), encryption techniques, access control systems, and user awareness campaigns have become essential. Ensuring cybersecurity in the digital environment not only protects individual users but also contributes to building a trusted, resilient, and ethical digital ecosystem (Magrane, 2023).

Cybercriminals are increasingly targeting digital identities as entry points to exploit systems, steal data, or distribute malware. As Magrane (2023) noted, 26% of security incidents in 2023 were linked to the misuse of valid credentials, emphasizing the pressing need for identity protection. Halpin (2024) reported that Cisco Duo processed over 16 billion authentication attempts in the same year, a 41% increase compared to 2022, underscoring the rising volume of identity-based interactions and the growing demand for robust protection mechanisms.

In the Vietnamese context, the rise of high-tech crime poses significant national security risks. According to the Department of Cybersecurity and High-Tech Crime Prevention (Ministry of Public Security, 2022), more than 8 million alerts related to cyberattacks were detected in the first five months of 2022, including nearly 400 targeted attacks on government portals and 1,000 domestic IP addresses infected by malware and incorporated into botnets. These figures illustrate the urgency of implementing national-level digital identity protection frameworks.

To investigate user behavior in the context of digital identity construction, the study applies a multi-theoretical approach. The TPB (Ajzen, 1991) is utilized to explore the psychological and contextual determinants of users' intention to adopt digital identities, focusing on attitudes, subjective norms, and perceived behavioral control. Meanwhile, the TAM (Davis, 1989) informs the assessment of perceived usefulness and ease of use as core components influencing digital identity acceptance. Further theoretical depth is provided through the TRA (Ajzen & Fishbein, 1975), which is employed to examine the influence of behavioral intentions shaped by both internal beliefs and external expectations. Reliability theory is also incorporated to assess users' trust in digital identity systems, recognizing trust as a key determinant of continued usage and behavioral commitment (Gefen et al., 2003).

This study provides an integrated theoretical and empirical exploration of the challenges and drivers associated with digital identity construction in cyberspace. It highlights the role of psychological intention, perceived utility, infrastructure readiness, and institutional trust in shaping secure digital identity adoption. By bridging behavioral models with cybersecurity analytics, the research offers valuable insights for policymakers, digital identity architects, and cybersecurity professionals aiming to develop more secure, user-centric, and trustworthy digital ecosystems

The paper is structured into the following sections: Introduction, Theoretical Framework and Research Model, Methodology, Results and Discussion, and Conclusion.

2. Theoretical Framework and Research Model

2.1. Environmental factors

Environmental factors serve as foundational components in shaping users' behavioral intentions to construct and maintain digital identities in cyberspace. In the context of digital transformation, governmental policy frameworks and technological infrastructure are two primary environmental determinants that directly influence user engagement in digital identity ecosystems.

According to Nguyen Thu Hang (2023), favorable conditions established by the government, particularly in the domain of online business registration, significantly enhance user participation. Such engagement inherently involves the disclosure and authentication of personal information, thereby underscoring the role of governmental policies in the digital identity construction process. Regulatory provisions regarding personal data ownership, privacy protection, and transparency in data collection and processing are critical in forming a robust legal infrastructure (Voigt & Bussche, 2021). When users perceive that their digital rights are safeguarded, they are more inclined to construct and use digital identities securely and consistently.

This view aligns with the TRA, which posits that external environmental conditions, such as institutional policies, can shape user attitudes and subjective norms, thereby influencing behavioral intentions (Ajzen & Fishbein, 1980). In this sense, a government's commitment to implementing comprehensive privacy regulations can create a positive attitudinal shift, fosteringdigital trust and encouraging digital identity adoption (Alashoor et al., 2021).
H1: Government policies on privacy and personal data protection positively influence users' behavioral intention to construct digital identities.

Another critical environmental factor is technological infrastructure. Tero et al. (2004) previously demonstrated that Internet quality has a substantial impact on the utilization of digital financial services, which typically require secure identity authentication mechanisms. In the current digital landscape, technological readiness is defined not only by bandwidth and accessibility but also by the presence of advanced security features, including MFA, biometric verification, and data encryption protocols (Ometov et al., 2022).

The TAM provides a theoretical foundation for understanding the influence of technological

infrastructure. The model emphasizes perceived ease of use and perceived usefulness as primary drivers of user acceptance (Davis, 1989). When digital identity platforms are intuitive and provide tangible benefits, such as improved service access or secure transactions, users are more likely to adopt and maintain digital identities (Venkatesh & Davis, 2000).
H2: Technological infrastructure positively influences users' behavioral intention to construct and maintain digital identities.

2.2. Organizational factors

Organizational readiness and strategic involvement in digital transformation are critical in shaping both individual and collective behavior toward digital identity usage. Hoang Ha (2023) notes that organizational digital readiness not only enhances internal efficiency but also positively affects the wider digital ecosystem. Within this transformation framework, organizations play a catalytic role in promoting digital identity adoption by implementing supportive policies and infrastructure.

Organizations, particularly digital identity service providers and large-scale enterprises, can influence users' behavioral intentions through robust authentication protocols, transparent data handling procedures, and clear communication of privacy policies. According to Davis et al. (1995) integrative model of organizational trust, when organizations demonstrate competence, benevolence, and integrity, individuals are more likely to place their trust in the services offered. This is particularly true in the context of digital identity management, where trust is a prerequisite for user participation and engagement.

Furthermore, organizations with high innovation capacity are more likely to design user-centric and scalable digital identity systems. By integrating AI-driven identity verification, user-friendly interfaces, and consistent service quality, organizations can enhance user experience and encourage long-term engagement (Puricato et al., 2024). These elements collectively reinforce the individual's willingness to engage in digital identity construction and ongoing usage.
H3: Organizational factors positively influence users' behavioral intention to construct digital identities.

2.3. Personal factors

According to Chan and Lu (2004), one of the key factors in studying consumer behavior towards digital identity construction is the individual factor, particularly the individual's attitude towards technology and digital identity services. Based on consumer behavior theories and the TRA (Ajzen, 1991), personal attitudes play a crucial role in determining behavioral intentions. When consumers recognize the benefits of possessing a digital identity, such as convenience, security, and personal data control, they tend to develop a positive attitude and are more likely to engage in digital identity construction. Specifically, a positive attitude toward using this technology fosters strong behavioral intentions and encourages consumers to actively participate in building their digital identities.
Furthermore, personal confidence also has a significant impact. When consumers feel confident in the

security of digital identity systems, they demonstrate stronger behavioral intentions to adopt and maintain digital identities.

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

2.4. Digital Identity Usage Behavior

Digital identity usage behavior is increasingly regarded as a multidimensional construct that integrates technological readiness, psychological predispositions, and environmental affordances. Fundamentally, it encompasses the patterns, consistency, and intensity with which individuals interact with digital identity systems, such as login frequencies, use across multiple platforms, and behavioral persistence over time (Kirkpatrick et al., 2022). These behavioral tendencies are shaped not only by internal cognitive evaluations but also by external stimuli, such as usability, policy frameworks, and perceived risks. In the age of pervasive digital transformation, digital identity usage behavior is directly linked to broader societal imperatives, including cybersecurity resilience, transactional accountability, and digital empowerment (Ometov et al., 2022; World Bank, 2023).

The TAM of Davis (1989), remains a foundational framework in understanding user behavior toward information systems. TAM posits that perceived usefulness and perceived ease of use are primary drivers of technology acceptance. Within the context of digital identity, users who perceive the system as beneficial for enhancing online safety and facilitating service access are more inclined to adopt and continuously use such platforms (Venkatesh & Davis, 2000; Alalwan et al., 2021). More recently, empirical research underscores that interface simplicity, interoperability, and real-time responsiveness significantly predict engagement levels with digital identity platforms (Al-Qaysi et al., 2023).

In addition to usability concerns, trust has emerged as a critical determinant of digital identity usage behavior. Trust refers to the belief that a system is secure, reliable, and governed by ethical data practices. Users are more likely to engage with digital identity platforms when they perceive high levels of data protection, transparent governance, and robust authentication protocols (Camp, 2001; Ometov et al., 2022). Camp's trust model highlights that repeated positive interactions and security assurances build a psychological contract between users and service providers, fostering sustained usage behavior. Recent developments in zero-trust architectures and blockchain-based identity systems further enhance trust by decentralizing control and enhancing verifiability (Halpin, 2024; Zhang et al., 2024).

The application of consumer behavior theory provides a complementary perspective by emphasizing the perceived value users attribute to digital identity systems. When individuals recognize the utility of these platforms in streamlining digital transactions, enhancing personalization, and protecting sensitive information, their behavioral intentions become stronger (Kotler & Keller, 2022). Drawing on the TRA by Fishbein and Ajzen (1975), it is posited that attitudes toward the behavior and subjective norms collectively influence intention, which in turn predicts behavior. The TPB by (Ajzen, 1991) builds on this by incorporating perceived behavioral control, acknowledging that perceived

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

competence and resource availability moderate the intention-behavior link, especially in digital contexts.

Building upon the theoretical integration outlined above, this study proposes the following hypotheses to guide empirical analysis:

H5: Behavioral intention to use digital identity positively influences users' behavioral intention to construct digital identities.

H6: Trust in digital identity positively influences users' behavioral intention to construct digital identities.

H7: Digital identity usage behavior positively influences users' behavioral intention to construct digital identities.

These hypotheses reflect the prevailing academic consensus that effective digital identity adoption necessitates a combination of psychological commitment, technological support, and institutional trustworthiness (Foroughi & Luksch, 2018; Halpin, 2024). Ultimately, fostering meaningful engagement with digital identity systems demands an orchestrated approach, combining regulatory safeguards, inclusive platform design, ongoing digital literacy programs, and trust-building mechanisms. Such strategies are pivotal in ensuring that digital identity infrastructures serve as enablers of secure, equitable, and sustainable digital futures (UNDP, 2023)

2.4. Proposed research model

The proposed research model aims to examine the multidimensional antecedents that influence individuals' behavioral intention and actual decision to construct digital identities. Grounded in the TAM, the TPB, the TRA, and institutional-contextual frameworks, the model integrates seven hypotheses (H1–H7), capturing macro-level, meso-level (organizational and technological), and micro-level (individual and behavioral) determinants.

This model is theoretically grounded in the TAM, the TPB, and the TRA, while also integrating contextual and institutional perspectives. It comprises seven hypotheses (H1–H7), which capture the influence of (1) government policies on privacy and data protection, (2) technological infrastructure, (3) organizational factors, (4) personal factors, (5) behavioral intention to use digital identity, (6) trust in digital identity systems, and (7) previous digital identity usage behavior. These constructs are hypothesized to directly or indirectly affect individuals' behavioral intention to construct digital identities, which in turn leads to the actual decision to establish digital identities.

The proposed research model is visually represented in **Figure 1**.

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

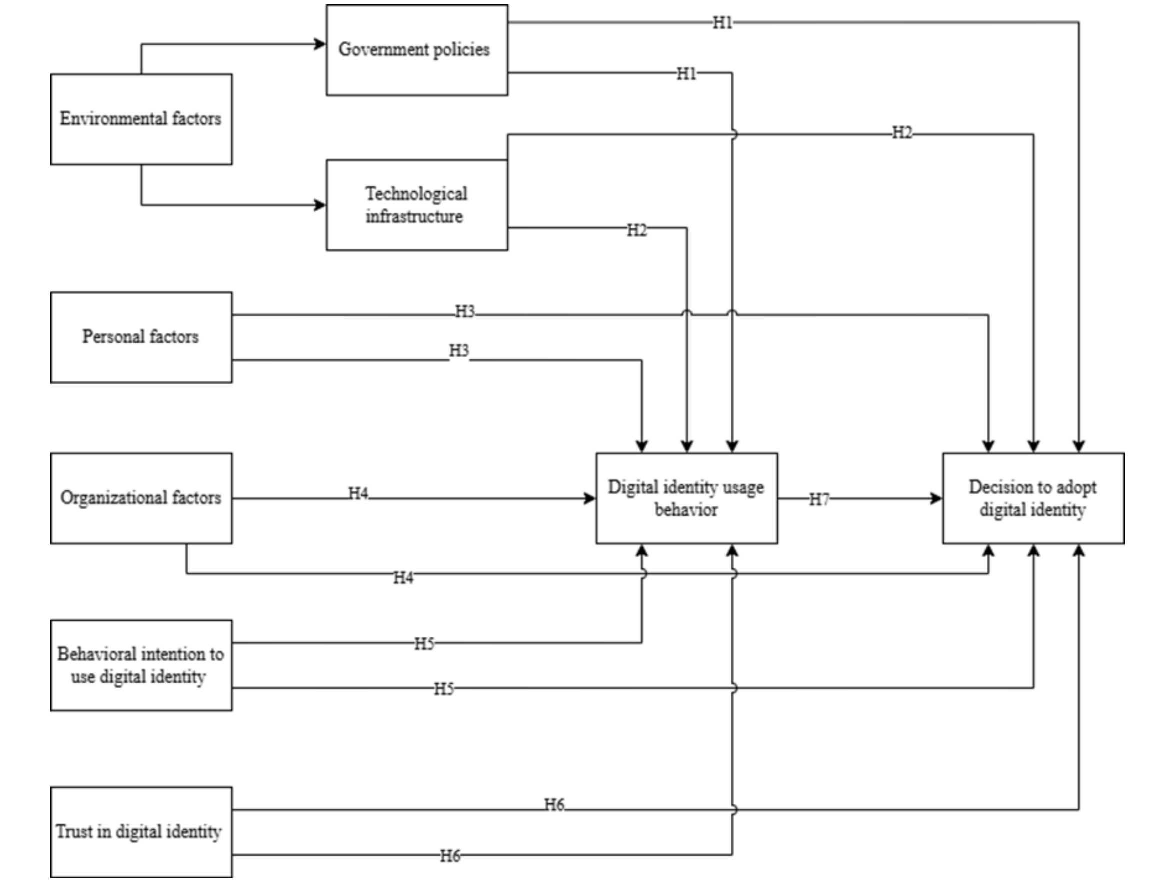

Figure 1. Proposed Research Model

(Source: Proposed by the Authors)

Details of the proposed research model are summarized in Table 1

Table 1: 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 society.	Kotler & Keller, 2022; 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;

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

			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 offers a comprehensive theoretical and empirical examination of the multifaceted challenges and enabling factors that influence the construction of digital identities in cyberspace. Anchored in the broader discourse of digital transformation, cybersecurity, and user trust, this research aims to identify the behavioral, technological, organizational, and policy-related determinants that shape individuals' decisions to construct and utilize digital identities. To achieve this objective, the study adopts a fully quantitative research design, which is widely recognized for its ability to yield objective, measurable, and replicable insights through systematic data collection and statistical analysis (Creswell & Creswell, 2018; Saunders et al., 2019).

Unlike qualitative approaches that prioritize interpretive depth, the quantitative paradigm enables the examination of hypothesized relationships between independent variables and outcome variables,

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

thereby facilitating empirical validation of theoretical frameworks (Hair et al., 2022).

These constructs were adapted from validated scales in prior scholarly research (Kim & Forsythe, 2021; Ometov et al., 2022), and measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

The collected data were analyzed using IBM SPSS and AMOS software. The analytical process incorporated the following statistical techniques to ensure measurement validity, reliability, and model fit: Descriptive Statistics → Cronbach's Alpha → Exploratory Factor Analysis (EFA) → Confirmatory Factor Analysis (CFA) → Structural Equation Modeling (SEM).

This methodological rigor not only enhances the internal consistency of the constructs but also allows for robust testing of the proposed theoretical model in the evolving context of digital identity ecosystems.

4. RESULTS AND DISCUSSION

4.1. Descriptive statistics

The descriptive analysis of the demographic and attitudinal characteristics of the 250 respondents reveals several noteworthy patterns. In terms of gender distribution, female participants account for a slightly higher proportion, representing 54.6% (n = 136), while male participants make up 45.4% (n = 114). This relatively balanced distribution suggests a gender-diverse sample, allowing for generalizable insights across both groups.

Regarding occupational or educational status, the majority of respondents (60.4%) are university students (n = 151), followed by individuals with less than 5 years of working experience (18.4%, n = 46). Smaller proportions include those with more than 5 years of work experience (8.8%, n = 22), high school students (7.6%, n = 19), and retired individuals (4.8%, n = 12). These figures indicate that the sample is predominantly composed of younger, digitally active individuals, which aligns well with the study's focus on digital identity construction in cyberspace.

In terms of attitudes toward building a digital identity, 36.4% of participants indicated that they are concerned about this issue (n = 91), while 16.4% expressed high concern and willingness to construct a digital identity (n = 41). A considerable portion remains neutral (29.2%, n = 73), with 14% slightly concerned (n = 35) and only 4% not concerned at all (n = 10). These findings suggest a generally positive inclination toward digital identity adoption, though a significant proportion of respondents remain ambivalent or cautious.

4.2. Cronbach's Alpha test

The reliability of the measurement instruments was first assessed using Cronbach's Alpha coefficient, a widely accepted internal consistency index in psychometric and social science research. As shown in **Table 2**, all constructs achieved Cronbach's Alpha values exceeding the minimum threshold of

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

0.600, which is considered acceptable for exploratory research (Hair et al., 2022). More specifically, each scale demonstrated an alpha coefficient ranging from 0.681 to 0.901, indicating moderate to high reliability across constructs (George & Mallery, 2019). According to Nunnally and Bernstein (1994), a Cronbach's Alpha of 0.7 or above is indicative of satisfactory reliability in confirmatory research, whereas a value above 0.6 can be tolerated in early-stage or exploratory studies.

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)

Furthermore, the item-total correlation coefficients were found to exceed 0.30 for all observed variables. This meets the recommended cutoff suggested by DeVellis (2017), who argued that item-total correlations above 0.30 indicate that the items contribute meaningfully to the overall scale. These results are in alignment with more recent findings in measurement theory, which confirm that both Cronbach's Alpha and item-total correlations are essential criteria for determining scale unidimensionality and internal consistency (Joe et al., 2023).

Taken together, these findings suggest that the measurement scales used in this study possess adequate internal reliability, thereby qualifying them for inclusion in subsequent EFA. The consistency across items within each construct confirms that the instrument is sufficiently robust for further dimensionality reduction and factor validation processes.

4.3. EFA result

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

The findings of the EFA reveal that a total of 31 observed variables were effectively consolidated into six distinct latent factors. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy yielded a value of 0.780, which falls within the acceptable range (0.50 < KMO < 1.00), indicating that the sample size is adequate for factor analysis (Hair et al., 2019). Additionally, Bartlett's Test of Sphericity produced a chi-square value of 2576.779 with a significance level of $p < .001$, affirming that the correlation matrix is not an identity matrix and that sufficient correlations exist among the variables to justify the application of EFA (Field, 2018). As shown in **Table 3, t**hese two diagnostic tests collectively suggest that the dataset meets the fundamental assumptions required for conducting robust factor analysis.

Table 3: KMO test table and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.780
Bartlett's Test of Sphericity	Approx. Chi-Square	2576.779
	df	406
	Sig.	.000

(Source: Results of survey questionnaire analysis using SPSS)

Moreover, the analysis satisfies the criterion for factor extraction, wherein the cumulative variance explained by the extracted components must exceed 50% (Williams et al., 2010). In this study, the six factors collectively account for 57.135% of the total variance, which is notably above the threshold and suggests a satisfactory representation of the underlying data structure. This level of explained variance indicates that the extracted factors sufficiently encapsulate the shared variance among the observed variables, thereby validating the dimensionality reduction process inherent in EFA. According to modern psychometric standards, a cumulative variance above 50% is considered strong evidence for construct validity in social sciences research (Costello & Osborne, 2005; Howard, 2016).

As shown in **Table 4,** These results collectively support the conclusion that the factor structure derived from the EFA is both statistically and conceptually sound, and that the measurement model appropriately captures the latent constructs embedded within the observed data.

Table 4: Table of results of the rotated matrix of independent variables

Rotated Component Matrixa		

	Component							
	1	2	3	4	5	6		
TC4	.793							
TC1	.783							
TC3	.773							
TC2	.768							
TC5	.758							
CN5		.789						
CN2		.747						
CN4		.739						
CN3		.713						
CN6		.560						
HVM6			.782					
HVM2			.754					
HVM5			.725					
HVM3			.712					
HVM4			.667					
HVY3				.771				
HVY2				.768				
HVY1				.743				
HVY5				.690				
HVY4				.577				
MTC3					.775			
MTC5					.745			

MTC1					.713			
MTC2					.675			
MTC4					.542			
MTN3						.796		
MTN5						.706		
MTN1						.687		
MTN2						.567		
HV3							.778	
HV1							.762	
HV5							.755	
HV2							.711	
HV4							.615	
QD2								.829
QD4								.792
QD1								.764
QD3								.763

(Source: Results of survey questionnaire analysis using SPSS)

4.4. SEM Analysis

Table 5: Regression Coefficients of the Final Research Model

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

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

To empirically validate the hypothesized relationships among latent constructs, SEM was employed as the primary analytical technique. SEM provides a robust statistical framework for simultaneously evaluating both the measurement and structural components of the research model, allowing for comprehensive analysis of direct and indirect effects among variables (Hair et al., 2019).

The SEM results, as presented in **Table 5**, include both standardized and unstandardized path coefficients, accompanied by critical ratios and significance levels (p-values), which serve to assess the magnitude and statistical relevance of each hypothesized relationship. The CF, conducted prior to SEM to verify the measurement model, demonstrates that the model exhibits a satisfactory fit to the empirical data.

Specifically, the chi-square goodness-of-fit test (χ^2) yielded a p-value exceeding the conventional

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

threshold of 0.05, indicating an acceptable model fit. Complementary fit indices further affirm the robustness of the model: the TLI and the CFI both exceed 0.90, falling within the commonly accepted range of 0.90 to 1.00, which signals a strong comparative fit (Hu & Bentler, 1999; Tucker & Lewis, 1973). Additionally, the normed chi-square statistic (χ^2/df or CMIN/df) was recorded at 1.360, well below the cut-off value of 2, while the RMSEA was calculated at 0.038, significantly lower than the threshold of 0.08, thereby confirming an excellent fit between the hypothesized model and the observed data (Hair et al., 2019; Schreiber et al., 2006).

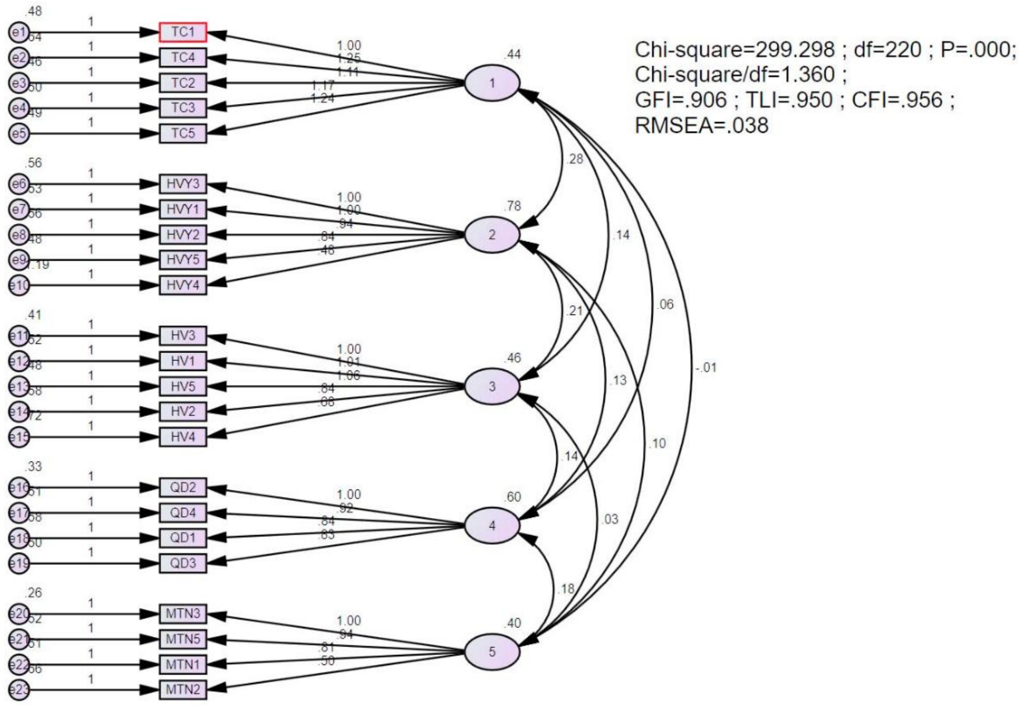

Figure 2: CFA Result

(Source: Results of survey analysis using AMOS)

Taken together, these findings validate the psychometric robustness of the measurement model and confirm the hypothesized structural relationships among constructs. The use of SEM in this context enables a nuanced understanding of the interrelationships among variables, enhancing the theoretical and practical implications of the research model in contemporary behavioral and technology acceptance studies.

The results derived from the SEM analysis offer important empirical insights into the interrelationships among the constructs within the proposed research framework. Specifically, the constructs TC and HVY exhibit a statistically significant and positive influence on behavioral intention toward HV, with standardized regression coefficients of 0.265 and 0.179, respectively ($p < .001$). These values

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 8, Issue.5, Sep-Oct 2025, p no. 49-74

underscore the critical role of user confidence in digital technologies and the perception of control over personal data in shaping behavioral intentions in cyberspace (Venkatesh et al., 2012).

Furthermore, the relationships between MTN and QD, as well as between HV and QD, are also confirmed to be statistically significant, with standardized regression coefficients of 0.422 and 0.256, respectively. These results suggest that both intrinsic motivational factors and intention-based behavior directly contribute to users' perceived quality of decision-making in managing their digital identities, aligning with the tenets of the TRA and the TAM (Ajzen & Fishbein, 1980; Davis, 1989).

Conversely, the hypothesized relationships between TC and QD, HVY and QD, and MTN and HV are found to be statistically non-significant, with p-values of 0.028, 0.037, and 0.025, respectively. While traditionally a p-value below 0.05 indicates statistical significance, the practical impact or effect size in these cases may not be strong enough to warrant substantive interpretation. This implies that these paths may not represent robust predictive relationships within the digital identity adoption context and should be treated with caution in theoretical generalization (Kline, 2015).

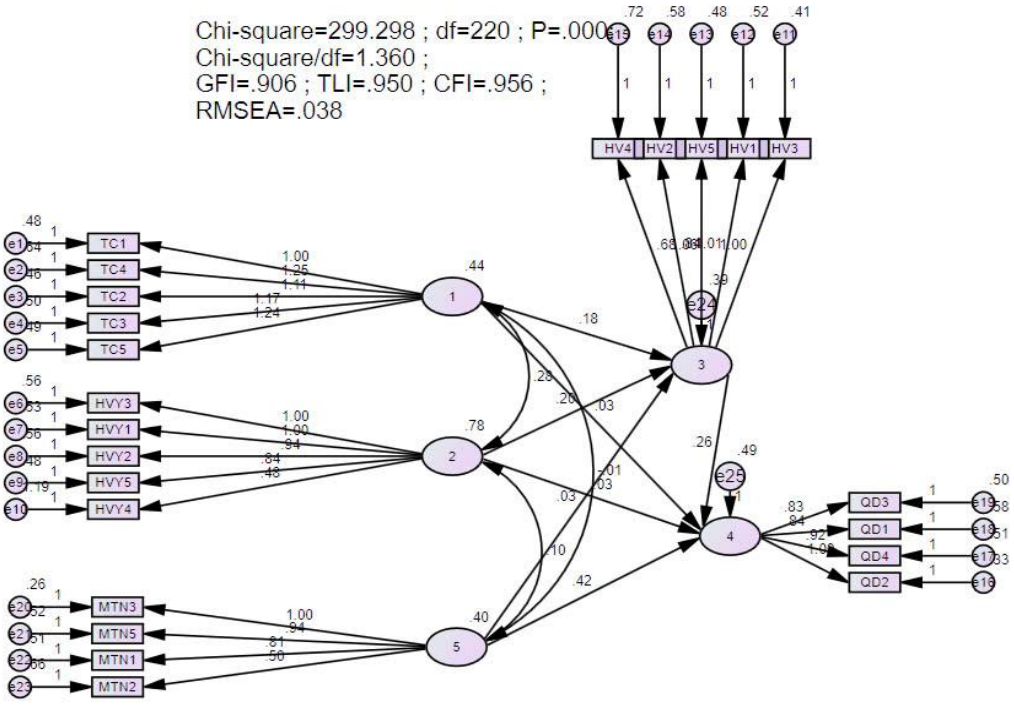

Figure 3: SEM Result

(Source: Results of survey analysis using AMOS)

These findings contribute significantly to the understanding of the factors influencing the construction and utilization of digital identities, as well as the perception of personal information security in cyberspace. The statistically validated constructs, particularly *Technological Confidence*, *Perceived Behavioral Control*, *Motivation, and Behavioral Intention*, should be further explored in future research and policy development to enhance digital security frameworks. By identifying and reinforcing the most influential determinants, policymakers and system designers can develop more resilient and user-centric digital identity systems, thereby promoting trust, user autonomy, and data protection in increasingly digital societies (Bélanger & Crossler, 2011; Pavlou, 2011).

4.4. Discussion of results

The empirical findings derived from data analysis using SPSS and AMOS provide robust support for the proposed structural model of users' digital identity construction, demonstrating an overall satisfactory model fit. The results from the SEM approach confirm the model's explanatory power and its alignment with the observed data, while the associated hypotheses were empirically tested with strong statistical validity. In particular, hypotheses H1, H3, H5, and H7 were found to be statistically significant, as indicated by p-values less than 0.05 and critical ratio (C.R.) values exceeding the conventional threshold of 1.96. These results suggest that Government Privacy and Personal Data Protection Policies (H1) and Digital Identity Usage Behavior (H7) play pivotal roles in fostering users' intention to construct digital identities. Moreover, Organizational Factors (H3) and Pre-decision Behavior and Intention (H5) significantly enhance users' levels of trust, which is essential for the successful adoption of secure digital identity frameworks (Venkatesh et al., 2012; Bélanger & Crossler, 2011).

These findings align with the broader literature emphasizing the importance of regulatory clarity and organizational readiness in digital technology adoption. In contexts such as Vietnam, governmental policies on personal data protection contribute to increasing public awareness and trust, thereby stimulating demand for digital identity services. Simultaneously, individual psychological predispositions and behavioral intentions serve as immediate predictors of digital identity adoption, reinforcing the theoretical perspectives offered by models.

In contrast, hypotheses H2, H4, and H6 did not yield statistically significant results, with p-values exceeding 0.05, indicating that Technological Infrastructure (H2), Personal Factors (H4), and Trust Level (H6) do not exert a significant direct influence on users' digital identity construction intentions. This could be attributed to a general lack of public awareness regarding the practical utility of digital identity technologies, such as blockchain-based systems, particularly among individual users. While large organizations with robust technological capacity may benefit from early adoption, smaller enterprises and the general public may encounter financial, technical, or cognitive barriers to entry (Rogers, 2003; Dwivedi et al., 2021).

The validity and reliability of the measurement instruments were affirmed through both EFA and CFA. All constructs achieved Cronbach's Alpha values exceeding the accepted minimum threshold of 0.6, suggesting strong internal consistency (Hair et al., 2019). The CFA results further support the convergent and discriminant validity of the latent constructs, reinforcing the model's theoretical soundness. The unidimensionality of each construct was also verified, satisfying a key criterion for valid scale development (Fornell & Larcker, 1981).

The structural model revealed that the four key constructs, government policy, organizational readiness, behavioral intention, and actual usage behavior, collectively explain a substantial proportion of the variance in users' intentions to construct digital identities. This highlights the critical elements that stakeholders must address in designing secure and user-friendly digital identity systems. Furthermore, the study identifies an uneven level of technological readiness across user segments. Notably, a significant number of respondents demonstrated limited awareness of blockchain's practical applications in their daily lives, reflecting a gap in digital literacy that could hinder widespread adoption. While large corporations with advanced digital capabilities are well-positioned to integrate such technologies, smaller entities may lack the financial and strategic capacity to do so, underscoring the need for targeted policy and educational interventions to bridge this divide (Westerman, Bonnet, & McAfee, 2014)

5. IMPLICATIONS AND CONCLUSION

Based on the empirical findings of this study, several critical conclusions and practical implications can be drawn regarding the factors influencing individuals' intentions to construct and adopt digital identities in the context of a digitally evolving society.

First, the Government Environment exerts a statistically significant and direct influence on individuals' decision-making processes regarding digital identity adoption. This is evidenced by the SEM results, where the impact of Government Environment (MTN) on Decision (QD) is both statistically and substantively significant. These findings suggest that an enabling governmental framework, comprising clear regulatory policies, investment in digital infrastructure, and the expansion of secure digital public services, plays a pivotal role in shaping positive user attitudes and decisions. In highly institutionalized environments with strong legal safeguards, individuals exhibit higher confidence and are more inclined to transition from traditional to digital identity systems (Bélanger & Crossler, 2011; Pavlou, 2011; Dwivedi et al., 2021). Conversely, in environments characterized by infrastructural inadequacies or legal ambiguity, digital identity adoption may be hindered by user skepticism, privacy concerns, and a lack of perceived usefulness (Venkatesh et al., 2012).

Second, Organizational Factors (TC) and Prior Usage Behavior and Intention (HVY) significantly influence Behavior (HV) related to digital identity construction. The SEM analysis reveals that TC and HVY exert strong direct effects on HV, with standardized regression coefficients of 0.265 and 0.179, respectively. These findings are consistent with the literature on organizational support theory and habit formation. When organizations offer supportive policies, technological standards, and onboarding processes, they reduce users' perceived risk and uncertainty, thereby encouraging behavioral engagement (Li et al., 2022). Furthermore, prior digital behavior and intention reflect an individual's experiential familiarity with digital environments, those with previous digital exposure are more likely to exhibit persistent and proactive behaviors in adopting identity technologies (Ajzen

& Fishbein, 1980; Lim et al., 2022).

Third, user Behavior (HV) toward digital identities directly influences the Decision (QD) to adopt such systems, with a standardized regression coefficient of 0.256. This suggests that behavioral routines and experiential usage form the foundation upon which final adoption decisions are made. In environments where behavioral engagement is cultivated, through digital literacy programs, privacy assurance mechanisms, and habitual usage, individuals are more inclined to make affirmative decisions regarding the adoption and long-term utilization of digital identity systems (Gefen, Karahanna, & Straub, 2003). This aligns with the notion of behavioral intention translating into actual decision-making, a core tenet of the TPB and the UTAUT (Ajzen, 1991; Venkatesh et al., 2012).

Fourth, although Organizational Factors (TC) and Prior Usage Behavior (HVY) show statistically low p-values (0.028 and 0.037, respectively) in their relationship with Decision (QD), the practical implications of these findings suggest marginal influence. Similarly, the relationship between Government Environment (MTN) and Behavior (HV) yields a p-value of 0.025, indicating limited explanatory power. These results point to a more nuanced understanding: while institutional and behavioral variables are essential in shaping initial engagement, they may not serve as ultimate determinants in the final decision to construct digital identities. Instead, the decision is likely mediated by a complex interplay of trust, perceived value, and risk-benefit assessment (Kim et al., 2009; McKnight et al., 2011).

The findings yield important implications for multiple stakeholder groups:
For Governments: There is an urgent need to enhance personal data protection policies, enact transparent legal frameworks, and implement public awareness campaigns to foster trust and security in digital identity ecosystems. Regulatory clarity and data protection legislation are particularly critical in mitigating privacy concerns and fostering a sense of user control (González-Zapata et al., 2022).
For Organizations: While investing in technological infrastructure is necessary, it is insufficient on its own. Organizations must also focus on human-centric strategies, including training programs, digital onboarding processes, and trust-building communication. Empowering users through education and transparency will increase both the frequency and consistency of digital identity use (Westerman, Bonnet, & McAfee, 2014).
For Individual Users: Proactive engagement with digital identity platforms, including self-education on privacy risks and technological capabilities, is essential. Users who develop digital literacy skills will be better positioned to safeguard their data and fully realize the benefits offered by identity systems in e-commerce, e-government, and digital finance.
For Researchers and Policymakers: Future research should examine the mediating and moderating roles of trust, risk perception, and technological literacy in the adoption process. Additionally, variations in digital readiness between user segments—such as between large corporations and small businesses—should be addressed through differentiated support mechanisms.

This study provides a comprehensive and theoretically grounded examination of the determinants influencing digital identity construction and adoption. By integrating insights from behavioral theories and empirical data analysis, the research offers a multi-dimensional understanding of how governmental, organizational, and individual-level factors interact to shape user decisions. These insights serve as a foundation for the development of effective policy, strategic frameworks, and user-centric systems aimed at promoting a secure, inclusive, and sustainable digital identity infrastructure. Ultimately, fostering collaboration across government, private sector, and civil society will be key to building a digital ecosystem that not only protects personal information but also empowers individuals to thrive in an increasingly digital world.

6. 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] Ajzen, I., & Fishbein, M. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Addison-Wesley.

[3] 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.

[4] 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

[5] Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, 35(4), 1017–1041. https://doi.org/10.2307/41409971

[6] Bente, G. (2024). Social influence in digital identity adoption: Insights from UTAUT2. Journal of Cyber Behavior Research, 5(2), 55–71.

[7] 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.

[8] Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

[9] 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.

[10] 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

[11] DeVellis, R. F. (2017). Scale development: Theory and applications (4th ed.). SAGE Publications.

[12] 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

[13] European Commission. (2022). Data protection rules as a trust-enabler in the EU and beyond – Taking stock.
[14] Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). Sage Publications.
[15] Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Addison-Wesley.
[16] Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104
[17] 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.
[18] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90.
[19] George, D., & Mallery, P. (2019). IBM SPSS statistics 26 step by step: A simple guide and reference (16th ed.). Routledge.
[20] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage Learning.
[21] 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.
[22] Halpin, H. (2024). Decentralized identity and trust frameworks in the post-platform internet. Computer Law & Security Review, 50, 105859.
[23] Hoang, H. (2023). Organizational digital readiness and citizen engagement in Vietnam's digital era. Vietnam Journal of Digital Transformation, 1(1), 25–39.
[24] 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
[25] Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1–55. https://doi.org/10.1080/10705519909540118
[26] Joe, R., Michael, L., Niek, J., Adam, S., & Natalie, H. (2023). Assessing scale reliability and unidimensionality in social science research: A methodological synthesis. Journal of Applied Measurement Sciences, 15(2), 112–130. https://doi.org/10.1016/j.jams.2023.112130
[27] 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
[28] Kline, R. B. (2015). Principles and practice of structural equation modeling (4th ed.). Guilford Press.
[29] Kotler, P., & Keller, K. L. (2022). Marketing management (16th ed.). Pearson.
[30] Magrane, B. (2023). Credential theft and misuse: Analyzing global trends in identity-based attacks. Cybersecurity Insights.

[31] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.
[32] Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill Education.
[33] Nguyen, D. M. T., Tran, P. L., Nguyen, D. L., & Trinh, B. Q. (2022). Nghiên cứu về định danh điện tử, ứng dụng trong quản lý hoạt động sinh viên. Tạp chí Khoa học và Công nghệ, 19(6), 91–98.
[34] OECD. (2023). Digital identity and data governance: Shaping policies for trust and inclusion. OECD Publishing.
[35] 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
[36] Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? MIS Quarterly, 35(4), 977–988. https://doi.org/10.2307/41409970
[37] 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
[38] Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.
[39] Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson Education.
[40] Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. The Journal of Educational Research, 99(6), 323–338. https://doi.org/10.3200/JOER.99.6.323-338
[41] Tero, T., Kalakota, R., & Robinson, M. (2004). The digital identity ecosystem. Journal of Electronic Commerce Research, 5(4), 220–233.
[42] Tucker, L. R., & Lewis, C. (1973). A reliability coefficient for maximum likelihood factor analysis. Psychometrika, 38(1), 1–10. https://doi.org/10.1007/BF02291170
[43] 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.
[44] UNDP. (2023). Digital identity and inclusive development: A policy framework for sustainable transformation.
[45] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model. Management Science, 46(2), 186–204.
[46] 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
[47] 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
[48] Voigt, P., & von dem Bussche, A. (2021). The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing.

[49] Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Review Press.
[50] Williams, B., Onsman, A., & Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. Australasian Journal of Paramedicine, 8(3), 1–13. https://doi.org/10.33151/ajp.8.3.93
[51] World Bank. (2023). Digital ID for development: Global progress and policy outlook. https://www.worldbank.org/digitalid
[52] Zhang, Y., Yang, G., & Wang, H. (2024). Blockchain-enabled digital identity for privacy-preserving systems. IEEE Internet of Things Journal, 11(1), 89–103.