The 3rd ASEAN School of Business Network International Conference 2026
www.aseansbn.org August 6-7, 2026 Pathum Thani, Thailand

Examining Digital Banking Usage Behavior among Generation Z in North Sumatra: The Mediating Role of Behavioral Intention

Arif Pratama Marpaung [1*]
[1]Universitas Muhammadiyah Sumatera Utara, Indonesia

*Corresponding Author: arifpratamamm@umsu.ac.id

ABSTRACT

The rapid advancement of digital technology has transformed the banking industry, accelerating the adoption of digital banking services worldwide. Despite the increasing use of digital banking, concerns regarding cybersecurity and trust remain critical factors influencing users' behavioral intentions and actual usage. This study examines digital banking usage behavior among Generation Z in North Sumatra by investigating the roles of cyber attack awareness, cyber security measures, trust in service providers, and trust in the internet, with behavioral intention serving as a mediating variable. A quantitative research design was employed A non-probability sampling approach. Data were collected from 327 Generation Z respondents through a structured questionnaire and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS. The results indicate that cyber attack awareness and cyber security measures significantly influence behavioral intention, which subsequently enhances digital banking usage behavior. In contrast, digital infrastructure trust does not demonstrate significant direct or indirect effects on digital banking usage behavior. Several relationships show marginal effects at the 10% significance level, indicating limited statistical evidence for specific pathways. The mediating role of behavioral intention is partially supported in explaining the relationships between cybersecurity-related factors, trust dimensions, and digital banking usage behavior. This study contributes to the digital banking literature by integrating cybersecurity awareness, cybersecurity measures, and trust into a comprehensive behavioral framework. The findings provide practical implications for financial institutions in strengthening cybersecurity strategies and fostering user trust to promote greater digital banking adoption among Generation Z in North Sumatra.

Keywords: Digital Banking Usage Behavior, Institutional Trust, Digital Infrastructure Trust, Generation Z.

DOI: https://doi.org/10.64458/asbnic.v3.129

INTRODUCTION

Digital transformation has made mobile banking, internet banking, and banking applications central to the relationship between banks and their customers. The mobile banking adoption literature consistently shows that perceived benefits, ease of use, compatibility, risk, security, and trust shape users'

decisions (Baptista & Oliveira, 2016; Jafri et al., 2024; Shaikh & Karjaluoto, 2015). In the North Sumatra banking context, Khofifah and Marpaung (2024) found that cyberattack risk, cybersecurity measures, transaction risk perception, and online banking usage are relevant factors in explaining customers' commitment to using banking services. Consequently, banks face a challenge that extends beyond attracting new users. They must also sustain usage after the initial adoption stage.

Generation Z provides a relevant context for examining this issue because much of this cohort's experience with financial services occurs through mobile devices and digital interfaces. Digital-only banking experiences among younger users are shaped by service functionality, experience quality, trust, and the compatibility of services with digital lifestyles (Windasari et al., 2022). However, frequent usage does not necessarily mean that users feel secure, understand cyber threats, or trust every component of a digital service.

The growth of digital transactions has increased users' exposure to phishing, social engineering, malware, identity theft, data misuse, and account takeover. Mobile banking studies show that security, privacy, risk, and trust are associated with the formation of usage intention (Hanif & Lallie, 2021; Merhi et al., 2019). Data security can also influence customer trust and intention to adopt FinTech services (Zhang et al., 2023). Security should therefore not be understood solely as a technical capability of the system. It is also a matter of user perception and behavioral response.

This study distinguishes between two dimensions of security. Cyber Threat Awareness refers to users' ability to recognize and understand cyber threats. Perceived Cybersecurity Protection refers to users' assessment of the ability of banks, applications, and security mechanisms to protect data and transactions. Previous research indicates that awareness of cyberattacks can affect trust and commitment, while perceived security can shape acceptance of digital services (Aboobucker & Bao, 2018; Bajwa et al., 2023). Nevertheless, security-related perceptions do not always translate directly into usage behavior.

This study also distinguishes between Institutional Trust and Digital Infrastructure Trust. Institutional Trust concerns confidence in the competence, integrity, and reliability of the service provider. Digital Infrastructure Trust concerns confidence in the applications, networks, systems, and structural assurances that support digital transactions. This distinction is important because users may trust a bank as an institution while remaining uncertain about network stability, application security, or the technological safeguards employed. The research gap has three dimensions. First, security and trust studies often focus on initial adoption, whereas most respondents in this study have used digital banking for a relatively long period. Second, previous studies frequently examine security and trust as direct predictors without explaining the intentional mechanism that links these perceptions to actual usage behavior. Third, trust in institutions and trust in digital infrastructure are often treated as a single general construct. This study addresses these gaps by positioning Behavioral Intention as a mediating mechanism leading to Digital Banking Usage Behavior.

This study aims to examine the direct effects of CTA, PCP, IT, and DIT on DBUB; the effects of these four constructs on BI; the effect of BI on DBUB; and the mediating role of BI. The study contributes by drawing on the intention-use mechanism of UTAUT2, incorporating more specific security and trust constructs, distinguishing between two forms of trust, and explaining the indirect pathways that shape digital banking usage behavior among Generation Z users in North Sumatra.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Theoretical Foundation

The Unified Theory of Acceptance and Use of Technology 2, or UTAUT2, serves as the principal theoretical foundation of this study. UTAUT2 proposes that behavioral intention is the most immediate mechanism driving use behavior in consumer technology contexts (Venkatesh et al., 2012). In this study, Behavioral Intention represents users' intention to use digital banking services, whereas Digital Banking

Usage Behavior represents their actual use of these services. Accordingly, both constructs are retained in line with their original meanings and measurement sources, rather than being redefined as secure intention or continuance behavior.

The application of UTAUT2 to mobile banking has received substantial empirical support. Baptista and Oliveira (2015) showed that UTAUT2 constructs explain mobile banking acceptance and are influenced by cultural context. Oliveira et al. (2014) extended adoption research by integrating UTAUT, task-technology fit, and initial trust. Alalwan et al. (2017) demonstrated that trust enhances the explanatory power of UTAUT2 in mobile banking adoption. Merhi et al. (2019) likewise identified security, privacy, and trust as important extensions of UTAUT2 across cultural settings. Abu-Taieh et al. (2020) emphasized the role of behavioral intention in continued intention, while Tariq et al. (2024) showed that behavioral intention links cognitive factors to actual digital banking usage.

Although UTAUT2 provides the main theoretical basis, this study does not include all of its original constructs. The model focuses on the behavioral mechanism most relevant to the research objective, namely the pathway from security and trust evaluations to intention and subsequently to behavior. This approach is consistent with research showing that mobile banking literature has developed through extensions of technology acceptance models that incorporate risk, security, quality, and trust (Baptista & Oliveira, 2016; Shaikh & Karjaluoto, 2015). The systematic review by Jafri et al. (2024) also identifies trust and security as central themes in banking-related FinTech adoption.

Post-adoption user experience remains important because usage behavior is shaped by users' evaluations of benefits, security, quality, and trust based on actual experience. Research on Generations Y and Z shows that digital-only banking experiences involve both functional and relational evaluations, rather than technology acceptance alone at the initial stage (Windasari et al., 2022). Continuance research also provides complementary evidence that trust, satisfaction, and post-adoption evaluations can sustain usage over time (Poromatikul et al., 2020; Talwar et al., 2020). In the present model, this literature provides contextual support, while the dependent construct remains defined as Digital Banking Usage Behavior.

Hypothesis Development

Cyber Threat Awareness reflects the extent to which users understand the forms of cyber threats, their potential consequences, and the actions required when cyber risks arise. Bajwa et al. (2023) found that cyberattack awareness can reduce online banking customers' trust and commitment, indicating that threat awareness can influence users' psychological responses. Vafaei-Zadeh et al. (2025) identified response efficacy, self-efficacy, privacy awareness, and fear of cyberattacks as important determinants of cybersecurity awareness. Hanif and Lallie (2021) also showed that perceived cybersecurity risk is an important determinant of intention to use mobile banking. These findings suggest that users who understand cyber threats evaluate their behavior more deliberately. Such awareness may influence behavior directly or may first shape usage intention.

H1: *Cyber Threat Awareness has a positive effect on Digital Banking Usage Behavior.*
H6: *Cyber Threat Awareness has a positive effect on Behavioral Intention.*

Perceived Cybersecurity Protection refers to the perception that a system and its service provider have adequate mechanisms to protect identities, data, accounts, and transactions Aboobucker and Bao (2018) showed that security, privacy, risk, trust, and website usability jointly explain internet banking acceptance. Merhi et al., (2019) found that perceived security, perceived privacy, and trust affect intention to use mobile banking in two national contexts. Zhang et al. (2023) linked data security to customer trust and FinTech adoption intention. In Tunisia, Abdennebi (2023) found that perceived security does not always have a direct effect on adoption intention, although trust mediates specific relationships within the model. The findings of Hanif and Lalli (2021), together with the system security characteristics examined by Chandio et al. (2017), indicate that users must understand and trust

protective mechanisms before these mechanisms can influence usage decisions. Perceived protection is therefore expected to strengthen both behavioral intention and usage behavior.

H2: *Perceived Cybersecurity Protection has a positive effect on Digital Banking Usage Behavior.*
H7: *Perceived Cybersecurity Protection has a positive effect on Behavioral Intention.*

Institutional Trust refers to the belief that a bank or service provider possesses the competence, integrity, benevolence, and ability to fulfill its commitments. Gefen et al. (2003) showed that trust can be integrated into technology acceptance models to reduce uncertainty in online transactions. Luo et al. (2010) positioned multidimensional trust and multifaceted risk as important factors in the initial acceptance of mobile banking. Lin (2011) showed that competence, benevolence, and integrity form knowledge-based trust, which influences attitudes and behavioral intention. Malaquias and Hwang (2016) confirmed the importance of trust in mobile banking use in developing countries. Gao and Waechter (2017) likewise demonstrated the role of initial trust in mobile payment adoption. Sharma and Sharma (2019) linked trust and quality dimensions to actual mobile banking usage. The meta-analysis by Kumar et al. (2023) showed that the relationship between trust and mobile banking varies across antecedents, outcomes, and cultural contexts. Based on this evidence, trust in the service provider is expected to influence both behavioral intention and usage behavior.

H3: *Institutional Trust has a positive effect on Digital Banking Usage Behavior.*
H8: *Institutional Trust has a positive effect on Behavioral Intention.*

Digital Infrastructure Trust concerns confidence in the security, privacy, application stability, network reliability, and structural assurances that enable digital transactions. Yousafzai et al. (2009) conceptualized trust as a multidimensional construct shaped by perceived security, perceived privacy, and perceived trustworthiness. Kesharwani and Bisht (2012) showed that trust and perceived risk influence internet banking adoption. Zhou (2012) explained that information quality, service quality, system quality, structural assurance, and reputation form initial trust. Aboobucker and Bao (2018) showed that the roles of security and trust may vary according to user conditions and service characteristics. This literature indicates that confidence in digital infrastructure can reduce uncertainty and support both behavioral intention and usage behavior.

H4: *Digital Infrastructure Trust has a positive effect on Digital Banking Usage Behavior.*
H9: *Digital Infrastructure Trust has a positive effect on Behavioral Intention.*

In UTAUT2, behavioral intention is a direct predictor of use behavior (Venkatesh et al., 2012). This relationship also appears in mobile banking and digital banking research. Tariq et al. (2024) showed that behavioral intention contributes to actual digital banking usage, while Abu-Taieh et al. (2020) demonstrated the relationship between intention and continued usage. Post-adoption studies further show that intention operates alongside users' evaluations of experience, usefulness, satisfaction, and trust in sustaining service usage (Foroughi et al., 2019; Poromatikul et al., 2020; Zhou, 2013). Based on this theory and evidence, Behavioral Intention is expected to be the most immediate mechanism driving Digital Banking Usage Behavior.

H5: *Behavioral Intention has a positive effect on Digital Banking Usage Behavior.*

The mediating role of BI is based on the premise that awareness, perceived protection, and trust do not always translate immediately into usage behavior. Users first form evaluations and intentions before using a service. Jafri et al. (2024), Alalwan et al. (2017), and Tariq et al. (2024) support the positioning of intention as a mechanism linking security or trust to financial technology usage. Post-adoption literature provides additional support by showing that psychological processes such as trust, satisfaction, confirmation, and interactivity can transmit the effects of service characteristics to usage decisions (Cao et al., 2018; Pokhrel & KC, 2024; Shao et al., 2019; Talwar et al., 2020; Yin & Lin, 2022). Therefore, BI is expected to mediate the relationships between CTA, PCP, IT, and DIT and DBUB.

H10: *Behavioral Intention mediates the effect of Cyber Threat Awareness on Digital Banking Usage Behavior.*
H11: *Behavioral Intention mediates the effect of Perceived Cybersecurity Protection on Digital Banking Usage Behavior.*
H12: *FBehavioral Intention mediates the effect of Institutional Trust on Digital Banking Usage Behavior.*
H13: *Behavioral Intention mediates the effect of Digital Infrastructure Trust on Digital Banking Usage Behavior.*

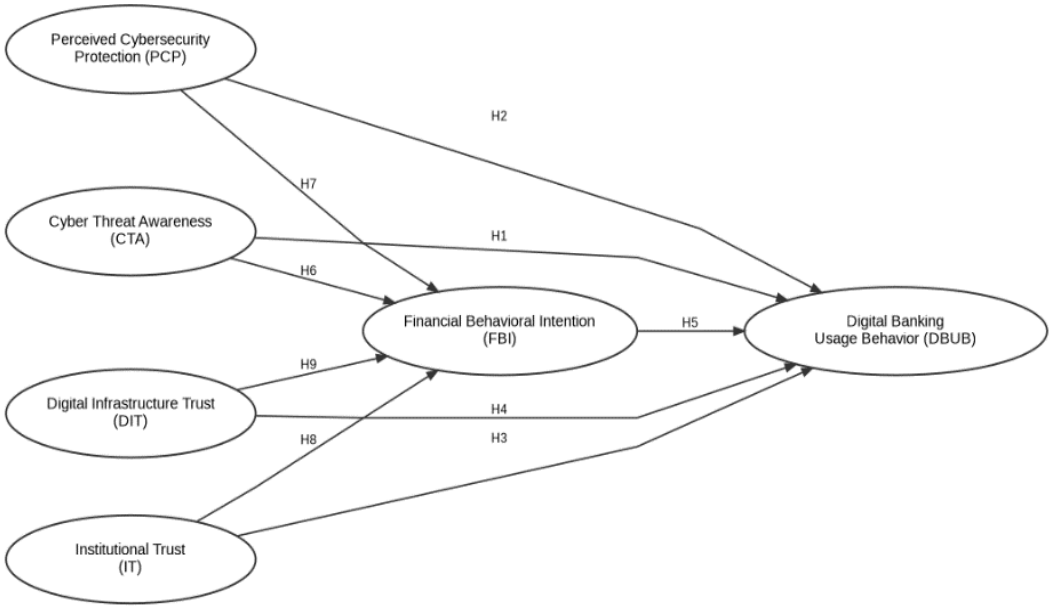


Figure 1. Research Model

METHOD

This study employed an explanatory quantitative design. The study population comprised Generation Z users of digital banking services in North Sumatra. A non-probability sampling approach was applied, with respondents selected based on predetermined eligibility criteria. The questionnaire was distributed through online and offline channels to 350 respondents, and 327 complete responses were retained for analysis after data screening.

The research instrument consisted of 20 items. Digital Banking Usage Behavior was measured using three use behavior items adapted from Armansyah (2021). Cyber Threat Awareness was measured using three items adapted from Bajwa et al. (2023). Perceived Cybersecurity Protection was measured using three items based on the system security characteristics examined by Chandio et al. (2017), Institutional Trust and Digital Infrastructure Trust were each measured using four items adapted from Armansyah (2021). Behavioral Intention was measured using three behavioral intention items based on UTAUT2 (Venkatesh et al., 2012). The labels BI and DBUB were retained to remain consistent with the meanings of the constructs and their original measurement sources, while the empirical adequacy of the indicators was evaluated through the measurement model.

Data were analyzed using PLS-SEM with SmartPLS. PLS-SEM is appropriate for testing predictive models involving multiple latent constructs and mediation paths. The measurement model was evaluated using outer loadings and cross-loadings. An outer loading of 0.70 or higher served as the primary criterion for retaining an indicator, while the overall construct validity was also considered. The structural model was assessed using path coefficients, t-statistics, and p-values obtained through bootstrapping. A 5% significance level was used for primary evidence, while a 10% level was used to identify marginal evidence. Accordingly, p-values between 0.05 and 0.10 were interpreted cautiously as weaker support.

RESULTS

The respondents comprised 101 men, representing 30.89%, and 226 women, representing 69.11%. By age, 167 respondents were 18 to 20 years old, 146 were 20 to 23 years old, 10 were 24 to 26 years old, and 4 were 27 to 28 years old. Most respondents were students. A total of 101 respondents had used digital banking for more than three years, while 88 had used it for one to two years. This profile indicates that the sample was dominated by young users with prior experience using digital banking services.

Table 1. Respondent Characteristics

Characteristic	Category	Frequency	Percent
Gender	Male	101	30.89%
	Female	226	69.11%
Age	18-20 years	167	51.07%
	21-23 years	146	44.65%
	24-26 years	10	3.06%
	27-28 years	4	1.22%
Education	Junior high school	0	0%
	Senior high school	101	30.89%
	Bachelor's degree	226	69.11%
	Master's degree	0	0%
	Doctoral degree	0	0%
Occupation	Civil servant/Police/Military	2	0.61%
	Lecturer/Physician/State-owned enterprise employee/Accountant/Lawyer	4	1.22%
	Farmer/Laborer/Livestock farmer	1	0.31%
	Entrepreneur/Private-sector employee/Contract employee	24	7.34%
	Student	296	90.52%
Monthly Income	< Rp3.000.000	281	85.93%
	Rp3.000.000-Rp7.000.000	32	9.79%
	Rp7.000.000-Rp10.000.000	5	1.53%
	> Rp10.000.000	9	2.75%
Type of Banking Service Used	E-wallet/payment application	31	9%
	Mobile Banking/Internet Banking	67	20.49%
	Both	229	70.03%
Length of Digital Banking Use	< 6 months	74	22.63%
	6 months-1 year	64	19.57%
	1-2 years	88	26.91%
	> 2 years	101	30.89%
Weekly Frequency of Digital Banking Use	< 3 times	116	35.47%
	3-5 times	119	36.39%
	5-10 times	48	14.68%
	> 10 times	44	13.46%

Source: Research Data (2025)

The measurement model assessment showed that all outer loadings ranged from 0.713 to 0.922. These values met the 0.70 threshold, and all indicators were therefore retained for analysis. CTA3 had the lowest loading at 0.713, while DBUB2 had the highest loading at 0.922.

Table 2. Outer Loadings

Indicator	CTA	PCP	DBUB	BI	DIT	IT
CTA1	0.873					
CTA2	0.748					
CTA3	0.713					
PCP1		0.853				
PCP2		0.845				
PCP3		0.822				
DBUB1			0.789			
DBUB2			0.922			
DBUB3			0.905			
BI1				0.860		
BI2				0.877		
BI3				0.905		
DIT1					0.816	
DIT2					0.831	
DIT3					0.848	
DIT4					0.846	
IT1						0.847
IT2						0.871
IT3						0.840
IT4						0.768

Source: *SmartPLS Output (2025).*
Note: *CTA = Cyber Threat Awareness; PCP = Perceived Cybersecurity Protection; DBUB = Digital Banking Usage Behavior; BI = Behavioral Intention; DIT = Digital Infrastructure Trust; IT = Institutional Trust.*

Each indicator loaded more highly on its intended construct than on any other construct. These results support discriminant validity based on the cross-loading assessment.

Table 3. Reliability Test

Construct	Cronbach's Alpha	rho_A	Composite Reliability (rho_C)	AVE	Description
Cyber Threat Awareness (CTA)	0.712	0.844	0.823	0.61	Reliable
Perceived Cybersecurity Protection (PCP)	0.792	0.793	0.878	0.706	Reliable
Digital Banking Usage Behavior (DBUB)	0.845	0.876	0.906	0.764	Reliable
Behavioral Intention (BI)	0.856	0.862	0.912	0.776	Reliable
Digital Infrastructure Trust (DIT)	0.857	0.864	0.902	0.698	Reliable
Institutional Trust (IT)	0.851	0.856	0.9	0.693	Reliable

Source: SmartPLS Output (2025).

Based on Table 3, all constructs demonstrate satisfactory reliability and convergent validity. The Cronbach's alpha, rho_A, and composite reliability values for all constructs exceed the recommended

threshold of 0.70, indicating adequate internal consistency. Furthermore, all constructs exhibit AVE values above the recommended threshold of 0.50, confirming convergent validity. Therefore, all measurement items are considered reliable and valid for further structural model analysis.

Table 4. Heterotrait-Monotrait Ratio (HTMT)

Construct	CTA	PCP	DBUB	BI	DIT	TSP
Cyber Threat Awareness (CTA)	-					
Perceived Cybersecurity Protection (PCP)	0.522	-				
Digital Banking Usage Behavior (DBUB)	0.576	0.493	-			
Behavioral Intention (BI)	0.671	0.501	0.742	-		
Digital Infrastructure Trust (DIT)	0.702	0.504	0.593	0.667	-	
Institutional Trust (IT)	0.731	0.477	0.615	0.731	0.794	-

Source: *SmartPLS Output (2025)*

Discriminant validity was assessed using the Heterotrait-Monotrait ratio (HTMT). As presented in Table 4, all HTMT values were below the recommended threshold of 0.90, indicating adequate discriminant validity among the constructs. In particular, the relationship between Digital Infrastructure Trust and Institutional Trust showed the highest HTMT value (0.794), which remained below the threshold, confirming that these constructs represent empirically distinct concepts.

Table 5. Cross-Loadings

Indicator	CTA	PCP	DBUB	BI	DIT	IT
CTA1	0.873	0.390	0.541	0.625	0.599	0.593
CTA2	0.748	0.341	0.303	0.307	0.374	0.452
CTA3	0.713	0.336	0.227	0.301	0.402	0.466
PCP1	0.452	0.853	0.331	0.406	0.401	0.427
PCP2	0.339	0.845	0.385	0.347	0.278	0.298
PCP3	0.352	0.822	0.357	0.338	0.419	0.309
DBUB1	0.359	0.387	0.789	0.397	0.379	0.394
DBUB2	0.457	0.371	0.922	0.617	0.472	0.513
DBUB3	0.494	0.371	0.905	0.652	0.501	0.504
BI1	0.530	0.344	0.507	0.860	0.498	0.545
BI2	0.457	0.381	0.587	0.877	0.485	0.552
BI3	0.548	0.416	0.619	0.905	0.535	0.627
DIT1	0.512	0.368	0.367	0.417	0.816	0.510
DIT2	0.472	0.371	0.409	0.471	0.831	0.579
DIT3	0.528	0.351	0.497	0.550	0.848	0.604
DIT4	0.545	0.368	0.451	0.467	0.846	0.635
IT1	0.564	0.389	0.483	0.575	0.592	0.847
IT2	0.571	0.420	0.451	0.570	0.636	0.871
IT3	0.539	0.290	0.447	0.552	0.556	0.840
IT4	0.507	0.258	0.425	0.473	0.542	0.768

Source: SmartPLS Output (2025).

The structural model results are presented in Table 6. CTA had no direct effect on DBUB ($\beta = 0.075$; $p = 0.281$), and H1 was therefore not supported. PCP had a positive effect on DBUB at the 10% level ($\beta = 0.120$; $p = 0.052$), providing marginal support for H2. IT had no direct effect on DBUB ($\beta = 0.077$; $p = 0.310$),

and H3 was not supported. DIT also had no direct effect on DBUB (β = 0.118; p = 0.146), and H4 was not supported. BI had a positive and significant effect on DBUB (β = 0.437; p < 0.001), supporting H5.

CTA had a positive effect on BI (β = 0.187; p = 0.006), PCP had a positive effect on BI (β = 0.132; p = 0.034), and IT had a positive effect on BI (β = 0.383; p < 0.001). Thus, H6, H7, and H8 were supported. DIT affected BI at the 10% level (β = 0.135; p = 0.088), providing marginal support for H9.

The indirect-effect analysis showed that BI mediated the effect of CTA on DBUB (β = 0.082; p = 0.011), supporting H10. The mediating effect of PCP on DBUB was significant at the 10% level (β = 0.058; p = 0.058), providing marginal support for H11. BI mediated the effect of IT on DBUB (β = 0.167; p < 0.001), supporting H12. The indirect effect of DIT on DBUB was not significant (β = 0.059; p = 0.102), and H13 was not supported.

Table 6. Path Coefficients and Hypothesis Testing

Path	Original Sample (O)	Sample Mean (M)	STDEV	T Statistics	P Values	Decision
CTA -> DBUB	0.075	0.080	0.069	1.079	0.281	Not supported
PCP -> DBUB	0.120	0.120	0.062	1.943	0.052+	Weak support
IT -> DBUB	0.077	0.082	0.076	1.015	0.310	Not supported
DIT -> DBUB	0.118	0.123	0.081	1.454	0.146	Not supported
BI -> DBUB	0.437	0.424	0.077	5.704	<0.001	Supported
CTA -> BI	0.187	0.193	0.068	2.761	0.006	Supported
PCP -> BI	0.132	0.135	0.063	2.117	0.034	Supported
IT -> BI	0.383	0.385	0.082	4.652	<0.001	Supported
DIT -> BI	0.135	0.131	0.079	1.707	0.088+	Weak support
CTA -> BI -> DBUB	0.082	0.081	0.032	2.548	0.011	Supported
PCP -> BI -> DBUB	0.058	0.058	0.031	1.894	0.0582	Weak support
IT -> BI -> DBUB	0.167	0.161	0.040	4.165	<0.001	Supported
DIT -> BI -> DBUB	0.059	0.056	0.036	1.633	0.102	Not supported

Source: *SmartPLS Output (2025).*
Note: *+ = P < 0.10.*

Discussion

The findings show that security and trust factors explain Digital Banking Usage Behavior more consistently when they operate through Behavioral Intention. This pattern supports the UTAUT2 proposition that intention is the most immediate mechanism leading to use behavior (Venkatesh et al., 2012). BI had the largest direct coefficient on DBUB. Awareness, perceived protection, and trust therefore do not automatically change service usage behavior. These factors must first shape users' intention to use digital banking.

CTA had no direct effect on DBUB, but it affected BI and exerted a significant indirect effect. This result indicates that awareness of threats does not necessarily cause users to increase or reduce their usage immediately. Instead, awareness first shapes users' intentions and deliberations. This finding can be interpreted alongside Bajwa et al. (2023), who showed that cyberattack awareness can alter trust and commitment, and Vafaei-Vafaei-Zadeh et al. (2025), who highlighted the importance of response efficacy and self-efficacy in forming cybersecurity awareness. Jafri et al. (2024) also showed that the relationships among security, trust, and adoption often involve interconnected mechanisms. Among Generation Z

users, transactional needs and established digital habits may prevent awareness alone from directly changing usage behavior.

PCP affected BI and showed both direct and indirect effects on DBUB at the 10% significance level. This evidence was weaker than the effects of BI or IT and should therefore be interpreted cautiously. The finding is nevertheless consistent with Merhi et al. (2019), who found that perceived security and privacy affect intention, and Zhang et al. (2023), who linked data security to trust and FinTech adoption intention. However, Ben Abdennebi (2023) showed that perceived security does not always directly affect adoption intention in developing-country contexts. The mere presence of technical protection may therefore be insufficient. Users need to understand the benefits of security features, observe evidence of protection, and feel capable of using those features effectively.

IT had no direct effect on DBUB but was the strongest predictor of BI and produced a substantial indirect effect. This result indicates that trust in the bank shapes users' confidence and intention before translating into usage behavior. The pattern is consistent with Gefen et al. (2003), Lin (2011), and Gao and Waechterv(2017), who conceptualized trust as a mechanism that reduces uncertainty and promotes intention. Sharma and Sharma, (2019) also demonstrated a relationship between trust and actual mobile banking usage. Post-adoption research by Talwar et al. (2020) and Shao et al. (2019) further suggests that trust remains relevant after initial adoption. Thus, a bank's reputation and integrity matter, but their effect on usage behavior is primarily realized through intention.

DIT had only a marginal effect on BI and had neither a direct nor an indirect effect on DBUB. This finding suggests that users may regard networks, applications, and digital mechanisms as infrastructure that is simply expected to be available. Trust in infrastructure may therefore lack sufficient variation to explain behavior. This interpretation does not diminish the importance of technology. Yousafzai et al. (2009), Kesharwani & Bisht (2012), and Zhou (2012) identified security, privacy, structural assurance, and system quality as important antecedents of trust and intention. However, the meta-analysis by Kumar et al. (2023) emphasized that the effect of trust depends on cultural context and model specification. In this sample, institutional trust appears to be more closely related to users' decisions than the more abstract concept of infrastructure trust.

The strong effect of BI on DBUB is consistent with digital banking studies that identify behavioral intention as a predictor of actual usage (Tariq et al., 2024) and as a basis for continued usage decisions (Abu-Taieh et al., 2020). Post-adoption literature also indicates that intention operates alongside users' evaluations of experience, usefulness, satisfaction, and trust (Foroughi et al., 2019; Poromatikul et al., 2020; Zhou, 2013). In this model, BI functions as the principal behavioral mechanism linking evaluations of security and trust to DBUB.

This interpretation is also supported by evidence from Generation Z users in Medan. Marpaung et al., (2024) found that financial management behavior in the use of paylater services among Generation Z is influenced by ease of use, financial socialization, hedonic motivation, self-monitoring, and financial literacy as an intervening variable. Although their study examined paylater rather than digital banking, it supports the view that Generation Z financial behavior in digital financial services is shaped by behavioral, cognitive, and evaluative factors. Therefore, the strong role of Behavioral Intention in the present study is consistent with the broader pattern of digital financial behavior among Generation Z in North Sumatra

The mediation results reveal differences across CTA, PCP, IT, and DIT. BI transmitted the effects of CTA and IT, transmitted the effect of PCP only marginally, and did not transmit the effect of DIT. This pattern is consistent with research that positions psychological processes as mechanisms linking service characteristics to usage decisions. Cao et al. (2018) explained the role of trust transfer, Yin and Lin (2022) emphasized interactivity, and Pokhrel and KC (2024) identified satisfaction as a mediating mechanism. The present findings add that behavioral intention can connect awareness or institutional trust with usage behavior.

Overall, the findings position user responses as a central component of digital banking security. Users do not merely react to technical features. They assess threats, evaluate protection, place trust in providers, and then form intentions. The results for Generation Z users in North Sumatra show that extensive digital experience does not eliminate the need for trust and security. Instead, such experience may make users more selective in distinguishing trust in institutions from trust in infrastructure.

CONCLUSION

This study concludes that Behavioral Intention is the principal mechanism explaining Digital Banking Usage Behavior among Generation Z users in North Sumatra. The findings show that Cyber Threat Awareness has no direct effect on Digital Banking Usage Behavior, but affects it indirectly through Behavioral Intention. Perceived Cybersecurity Protection affects Behavioral Intention and receives direct and indirect support at the 10% significance level. Institutional Trust has no direct effect on Digital Banking Usage Behavior, but strongly affects Behavioral Intention and indirectly affects Digital Banking Usage Behavior. Digital Infrastructure Trust has only a marginal effect on Behavioral Intention and has neither a direct nor an indirect effect on Digital Banking Usage Behavior. Behavioral Intention has the strongest direct effect on Digital Banking Usage Behavior.

Theoretically, this study supports the intention-use mechanism of UTAUT2 by showing that intention is the most immediate mechanism leading to use behavior. The findings also show that security and trust factors do not always influence usage behavior directly. Cyber Threat Awareness and Institutional Trust operate mainly through Behavioral Intention, while Perceived Cybersecurity Protection shows weaker direct and indirect effects. Digital Infrastructure Trust does not significantly explain Digital Banking Usage Behavior. These results clarify the importance of distinguishing trust according to its object. Trust in the banking institution has different behavioral consequences from trust in digital infrastructure.

This study contributes to the digital banking usage literature by examining security-related antecedents and two forms of trust within the intention-use mechanism. The contribution does not lie in introducing new constructs, but in explaining how Cyber Threat Awareness, Perceived Cybersecurity Protection, Institutional Trust, and Digital Infrastructure Trust shape usage behavior through Behavioral Intention. This finding is important because Generation Z users may frequently use digital banking without necessarily responding directly to cyber threats, protection features, or infrastructure quality.

From a managerial perspective, banks should transform security education from fear-based communication into actionable guidance. Banks should explain how users can identify phishing, protect one-time passwords and personal identification numbers, verify links, activate authentication features, and report incidents. Security communication should not only raise awareness, but also strengthen users' intention to use digital banking services responsibly. Banks should also make cybersecurity protection visible and easy to understand through clear information about authentication, transaction notifications, device controls, transaction limits, account recovery, and fraud-handling procedures.

The strong role of Institutional Trust indicates that banks must maintain integrity, transparency, reliability, and effective incident response. Banks should respond transparently to security incidents, provide timely complaint-handling services, clarify accountability, and maintain consistent communication with users. Although Digital Infrastructure Trust does not significantly affect usage behavior, this result should not be interpreted as a reason to neglect system quality. Application stability, network security, and data protection remain essential prerequisites, but these qualities must be translated into user experiences and evidence that users can clearly evaluate.

This study has several limitations. The data are cross-sectional and self-reported, which limits the ability to capture behavioral changes over time. The sample is restricted to Generation Z users in North Sumatra, so the findings may not fully represent other user groups or regions. Several relationships are supported only at the 10% significance level and therefore require cautious interpretation. Future

research may incorporate satisfaction, confirmation, incident experience, and actual transaction data to provide a stronger explanation of Digital Banking Usage Behavior.

REFERENCES

Abdennebi, H. Ben. (2023). M-banking adoption from the developing countries perspective: A mediated model. Digital Business, 3(2), 100065. https://doi.org/10.1016/j.digbus.2023.100065

Aboobucker, & Bao, Y. (2018). What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. The Journal of High Technology Management Research, 29(1), 109–123. https://doi.org/10.1016/j.hitech.2018.04.010

Abu-Taieh, E. M., AlHadid, I., Abu-Tayeh, S., Masa'deh, R., Alkhawaldeh, R. S., Khwaldeh, S., & Alrowwad, A. (2020). Continued intention to use of m-banking in Jordan by integrating UTAUT, TPB, TAM and service quality with ML. Journal of Open Innovation: Technology, Market, and Complexity, 8(3), 120. https://doi.org/10.3390/joitmc8030120

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. International Journal of Information Management, 37(3), 99–110. https://doi.org/10.1016/j.ijinfomgt.2017.01.002

Armansyah, R. F. (2021). Herd behavior in using mobile payment with Unified Theory of Acceptance and Use of Technology (UTAUT2). Jurnal Manajemen Dan Kewirausahaan, 23(3), 111–128. https://doi.org/10.9744/jmk.23.2.111-128

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. Information & Computer Security, 31(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. Computers in Human Behavior, 50, 418–430. https://doi.org/10.1016/j.chb.2015.04.024

Baptista, G., & Oliveira, T. (2016). A weight and a meta-analysis on mobile banking acceptance research. Computers in Human Behavior, 63, 480–489. https://doi.org/10.1016/j.chb.2016.05.074

Cao, X., Yu, L., Liu, Z., Gong, M., & Adeel, L. (2018). Understanding mobile payment users' continuance intention: A trust transfer perspective. Internet Research, 28(2), 456–476. https://doi.org/10.1108/IntR-11-2016-0359

Chandio, H. F., Irani, Z., Zeki, A. M., Shah, A., & Shah, S. C. (2017). Online banking information systems acceptance: An empirical examination of system characteristics and web security. Information Systems Management, 34(1), 50–64. https://doi.org/10.1080/10580530.2017.1254450

Foroughi, B., Iranmanesh, M., & Hyun, S. S. (2019). Understanding the determinants of mobile banking continuance usage intention. Journal of Enterprise Information Management, 32(6), 1015–1033. https://doi.org/10.1108/JEIM-10-2018-0237

Gao, L., & Waechter, K. A. (2017). Examining the role of initial trust in user adoption of mobile payment services: An empirical investigation. Information Systems Frontiers, 19(3), 525–548. https://doi.org/10.1007/s10796-015-9611-0

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+): A mixed-method study using modified UTAUT and MTAM with

perceived cyber security, risk, and trust. Technology in Society, 67, 101693. https://doi.org/10.1016/j.techsoc.2021.101693

Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2024). A systematic literature review of the role of trust and security on FinTech adoption in banking. Heliyon, 10(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

Kesharwani, A., & Bisht, S. S. (2012). The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. International Journal of Bank Marketing, 30(4), 303–322. https://doi.org/10.1108/02652321211236923

Khofifah, D., & Marpaung, A. P. (2024). Cyber Attack Risk in Commitment to use Banking Services: North Sumatra Evidance. Proceeding Medan International Conference on Economic and Business, 897–911.

Kumar, P., Chauhan, S., Gupta, P., & Jaiswal, M. P. (2023). A meta-analysis of trust in mobile banking: The moderating role of cultural dimensions. International Journal of Bank Marketing, 41(6), 1207–1238. https://doi.org/10.1108/IJBM-02-2022-0075

Lin, H.-F. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. International Journal of Information Management, 31(3), 252–260. https://doi.org/10.1016/j.ijinfomgt.2010.07.006

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decision Support Systems, 49(2), 222–234. https://doi.org/10.1016/j.dss.2010.02.008

Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. Computers in Human Behavior, 54, 453–461. https://doi.org/10.1016/j.chb.2015.08.039

Marpaung, A. P., Wardani, K. S., & Sani, A. (2024). Determinan Perilaku Pengelolaan Keuangan Dalam Penggunaan Paylater: Studi Kasus Pada Generasi Z Di Kota Medan. Value : Jurnal Manajemen Dan Akuntansi, 19(3), 857–874.

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. Technology in Society, 34(5), 101151. https://doi.org/10.1016/j.techsoc.2019.101151

Oliveira, T., Faria, M., Thomas, M. A., & Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. International Journal of Information Management, 34(5), 689–703. https://doi.org/10.1016/j.ijinfomgt.2014.06.004

Pokhrel, L., & KC, A. (2024). Mobile banking service quality and continuance intention: Mediating role of satisfaction: A two-stage structural equation modeling-artificial neural network approach. International Journal of Bank Marketing, 42(3), 389–413. https://doi.org/10.1108/IJBM-11-2022-0512

Poromatikul, C., Maeyer, P. De, Leelapanyalert, K., & Zaby, S. (2020). Drivers of continuance intention with mobile banking apps. International Journal of Bank Marketing, 38(1), 242–262. https://doi.org/10.1108/IJBM-08-2018-0224

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. Telematics and Informatics, 32(1), 129–142. https://doi.org/10.1016/j.tele.2014.05.003

Shao, Z., Zhang, L., Li, X., & Guo, Y. (2019). Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. Electronic Commerce Research and Applications, 33, 100823. https://doi.org/10.1016/j.elerap.2018.100823

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. International Journal of Information Management, 44, 65–75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

Talwar, S., Dhir, A., Khalil, A., Mohan, G., & Islam, A. K. M. N. (2020). Point of adoption and beyond: Initial trust and mobile-payment continuation intention. Journal of Retailing and Consumer Services, 55, 102086. https://doi.org/10.1016/j.jretconser.2020.102086

Tariq, M., Maryam, S. Z., & Shaheen, W. A. (2024). Cognitive factors and actual usage of FinTech innovation: Exploring the UTAUT framework for digital banking. Heliyon, 10(15), e35582. https://doi.org/10.1016/j.heliyon.2024.e35582

Vafaei-Zadeh, Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. International Journal of Bank Marketing, 43(3), 476–505. https://doi.org/10.1108/IJBM-03-2024-0138

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.

Windasari, N. A., Kusumawati, N., Larasati, N., Amelia, & Puspasuci, R. (2022). Digital-only banking experience: Insights from gen Y and gen Z. Journal of Innovation & Knowledge, 7(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

Yin, L.-X., & Lin, H.-C. (2022). Predictors of customers' continuance intention of mobile banking from the perspective of the interactivity theory. Economic Research-Ekonomska Istraživanja, 35(1), 6820–6849. https://doi.org/10.1080/1331677X.2022.2053782

Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in Internet banking adoption. The Service Industries Journal, 9(5), 591–605. https://doi.org/10.1080/02642060902719958

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data Security, Customer Trust and Intention for Adoption of Fintech Services: An Empirical Analysis From Commercial Bank Users in Pakistan. Sage Open, 13(3). https://doi.org/10.1177/21582440231181388

Zhou, T. (2012). Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. Computers in Human Behavior, 28(4), 1518–1525. https://doi.org/10.1016/j.chb.2012.03.021

Zhou, T. (2013). An empirical examination of continuance intention of mobile payment services. Decision Support Systems, 54(2), 1085–1091. https://doi.org/10.1016/j.dss.2012.10.034