International Journal of Business and Sustainable Development (IJBSD)
Vol. 3 Issue 2, July – December 2026 (e-ISSN No. 3139-4752)
DOI:10.67948/ijbsd/v3.i2.3210

Cybersecurity and Customer Switching Intention in the Banking Sector of Rupandehi District

Roshani Acharya*

Abstract:
The rapid expansion of digital banking has increased concerns about protecting customers' personal and financial information. This study examined associations between five cybersecurity-related perceptions and customer switching intention in the banking sector of Rupandehi District, Nepal: perceived security, data privacy, cyberattack experience, trust in the bank's security system, and cybersecurity awareness. A quantitative cross-sectional survey of 297 banking customers recruited through convenience sampling was analysed using partial least squares structural equation modelling (PLS-SEM), importance-performance map analysis (IPMA), and necessary condition analysis (NCA). The model explained 77.6% of sample variance in switching intention (R-squared = 0.776). Table 10 reports statistically significant negative path coefficients for perceived security, data privacy, cyberattack experience, and trust; cybersecurity awareness had a positive but nonsignificant coefficient. These directions, particularly the negative cyberattack-experience coefficient and its conflict with the sample-mean column, require verification against the original output and construct coding. The cross-sectional findings should be interpreted as associations, not causal effects.

Keywords: Cybersecurity, Customer Switching Intention, Perceived Security, Data Privacy.

Roshani Acharya*
MBA-BF Scholar, Lumbini Banijya Campus, Butwal, Nepal
**Corresponding author*

1.INTRODUCTION

Over the last ten years, the banking sector has been increasingly transforming, with digital technologies developing at a fast pace. Banking services have become faster, more convenient and more accessible than ever before, thanks to internet banking, mobile banking, QR-based payment systems, cloud computing, artificial intelligence (AI) and other financial technologies. The adoption of digital channels for day-to-day financial transactions such as fund transfers, bill payment, online purchases, and account management has increased the number of customers using digital channels. These innovations have enhanced service delivery efficiency and customer convenience, but they have also increased banks vulnerability to numerous cybersecurity threats including phishing attacks, identity theft, malware, ransomware, unauthorized access to accounts, online fraud, and data breaches. With the evolution of digital banking, cybersecurity is not only a technical issue, but it is a strategic issue that directly affects customer confidence, trust and long-term relationships with financial institutions (Saibaba, 2024; Tran, 2025).

Today's digital environment customers expect banks to provide secure platforms that safeguard their personal and financial information. If customers see digital banking systems as reliable and able to prevent cyber threats, customers will be more willing to continue to use such services and continue in a relationship with their banks. Strong security features decrease the perceived risk, increase the trust, and increase the customer confidence toward digital financial services (Merhi et al., 2019; Lee et al., 2023; Nguyen & Dao, 2024. Our customers may lose trust in us because they are worried about cyber fraud and poor security. They are also concerned about their privacy and data being stolen. This makes them look for other banks to do business with. Since many

banks are competing with each other cybersecurity is very important for keeping our customers and making them loyal to our bank.

Digital banking has become really popular in Nepal over the few years. The commercial banks in Nepal offer digital services. These services include banking on your phone banking, on the internet paying with QR codes using wallets and transferring money electronically. These developments have been backed by government initiatives promoting financial inclusion and digital payment systems leading to greater adoption of electronic banking services across the country. But with the rise of digital banking has come a new set of concerns for customers around online fraud, phishing scams, unauthorized transactions, password theft, identity theft and data privacy. "The banking sector is moving more and more to digital channels, and customers are increasingly aware of the importance of cybersecurity.

Previous studies in Nepal have mainly focused on electronic banking adoption, service quality, customer satisfaction, customer loyalty and relationship management. Security, privacy, reliability and service quality are the key factors affecting customers' banking experience and their satisfaction (Adhikari, 2025; Regmi & Sah, 2025). Likewise, Karmacharya (2024) noted that customer trust and relationship management are essential in enhancing customer satisfaction and loyalty in Nepalese financial institutions. Studies in Rupandehi District also show that service quality is an important factor in improving customer satisfaction and loyalty in retail banking (Bhatt & Nepali, 2021; Timalsina, 2024). The studies give helpful insights into customer behaviour, but do not pay much attention to whether or not cybersecurity concerns have an impact on the decision of customers to leave their existing bank and switch to another bank.

There are a number of theoretical perspectives to explain the reasons for cybersecurity may influence the customer switching behaviour. The theory of Planned Behavior (Ajzen, 1991) states that behavioural intention is determined by an individual's attitudes, perceived behavioural control and subjective norms. In the digital banking context, when customers perceive that a bank's cybersecurity measures are not adequate, they can develop negative attitudes towards the bank and increase their intention to switch. Relationship Quality Theory says that trust, commitment and satisfaction are very important for long term relationships with customers. This is especially true for technology-based services. When a bank has cybersecurity customers feel safe and confident. This is because good cybersecurity reduces the risk that customers think they will face. It also makes them feel more confident when they use banking. On the hand bad cybersecurity can make customers lose trust. Relationship Quality Theory and good cybersecurity go hand in hand to keep customers happy and loyal to their bank and, to the banking services that the bank offers.

People around the world are studying how cybersecurity affects digital financial services. When customers feel that their information is safe, they are more satisfied. They like the service more. They are also more likely to keep using the service. This is because they trust the service and feel that their privacy is protected. Good cybersecurity makes customers trust the company more. They are more likely to stay with the company. Cybersecurity is very important for financial services. Cybersecurity helps customers trust financial services and this makes customers stay with digital financial services. Cybersecurity is a part of digital financial services and banks need to have good cybersecurity to keep customers safe. However, most of the existing studies have focused on the intention of customers to continue using digital banking services, not on the switching intention of customers as a behavioral outcome.

A similar pattern is observed in the Nepalese banking literature. Most of the previous studies are related to customer satisfaction, electronic banking adoption, service quality and customer loyalty

(Thapa, 2023; Bohara, 2024; Karmacharya, 2024; Regmi and Sah, 2025) .Service quality is often cited as comprising security and privacy, but research rarely investigates whether customers would switch banks because of cybersecurity concerns. Moreover, Rupandehi District is witnessing in increasing pace in the area of digital banking and competition among commercial banks, but there is little empirical evidence from the district. So, there are three major gaps in research. First, there is a conceptual gap as cybersecurity has rarely been examined as a direct predictor of customer switching intention. Secondly, there is a contextual gap as previous Nepalese studies have looked into customer satisfaction and loyalty, not switching behavior. Third, there is a geographical gap, as the empirical evidence from Rupandehi District.

These research gaps have important practical implications. Commercial banks continue to heavily invest in digital technologies and cybersecurity infrastructure, but customers remain concerned about cyber fraud, privacy breaches, transaction security and protection of personal information. Failure to address these issues properly can lead to a slow erosion of customer trust and a shift to competitor banks seen to offer better security. In the absence of empirical evidence on the effect of cybersecurity on customer switching intention in Nepal, banks and policy makers will face challenges in devising effective strategies to enhance customer trust and boost customer retention. Therefore, the study aims to explore the impact of cybersecurity on customer switching intention in the banking sector of Rupandehi District, Nepal. This study uses Theory of Planned Behavior and Relationship Quality Theory to examine the effect of perceived security, data privacy, cyberattack experience, trust in the bank's security system, and cybersecurity awareness on customers' intention to switch banks. This study bridges the identified conceptual, contextual and geographical gaps and contributes to the emerging literature on digital banking and cybersecurity and further provides practical recommendations to commercial banks, regulators and policymakers who are looking to improve cybersecurity practices, gain customer trust and develop long-term customer retention in the dynamic digital banking environment of Nepal.

1.1 Research question

RQ1: *How do perceived security, data privacy, cyberattack experience, trust in the bank's security system, and cybersecurity awareness affect customer switching intention in the banking sector of Rupandehi District?*

RQ2: *What is the necessary condition for achieving high level of customer switching intention in the banking sector of Rupandehi District.*

1.2 Objectives

RO1: *To examine the effect of perceived security, data privacy, cyberattack experience, trust in the bank's security system, and cybersecurity awareness on customer switching intention*

RO2: *To determine the necessary condition for acheieving high level of customer switching intention.*

2. LITERATURE REVIEW

The increasing use of digital banking has transformed the delivery of financial services and has changed customer expectations for security, privacy, and quality of service. With more and more banking transactions taking place on digital platforms, cybersecurity has become an important factor in influencing customer behaviour. Literature suggests that customers' perceptions about security, privacy protection, trust and prior cyber experiences may significantly influence their willingness to continue or discontinue the use of banking services. Customer satisfaction, loyalty and continuance intention have been widely studied in the past but little attention has been paid to

customer switching intention due to cybersecurity issues especially in developing economies like Nepal. In this section, the main theories and empirical evidence about cyber security and customer switching intention are discussed.

2.1 Theoretical Review

Several behavioural and relationship theories provide a good foundation for understanding the effect of cybersecurity on customers' switching intention in the banking industry. Ajzen's (1991) Theory of Planned Behavior (TPB) posits that an individual's intention to behave is based on attitude toward the behavior, subjective norms, and perceived behavioral control. For digital banking, customers assess the security of banking platforms before they decide to proceed with their relationship with a bank. And if they feel that the cybersecurity measures are not enough or that another bank offers a safer digital environment, their intention to switch is likely to increase. Thus, TPB is an appropriate theoretical framework to explain customers' perception of cybersecurity and switching decisions.

Trust theory is also an important explanation of customer behaviour in digital banking. Trust is the confidence that customers have that the bank can safeguard their personal information, financial assets and online transactions. Given that digital banking services are highly technology driven, customers are very dependent on the reliability and security of the banking systems. Prior studies have repeatedly proven that higher cybersecurity increases customers' trust and commitment, and therefore increases customers' retention (Merhi et al., 2019; Panditharathna et al., 2024). Likewise, Nguyen and Dao (2024) also found that trust has a significant effect on customers' intention to continue to use the mobile banking service. The results suggest that trust is an important mechanism through which cybersecurity affects customer behaviour. According to the Perceived Risk Theory, customers assess the risks involved in using digital banking services before making any behavioral decisions. The perceived risk includes concerns about financial loss, identity theft, unauthorized transactions, privacy breaches and cyber fraud. "Higher perceived risk will lower customer confidence and increase the chance of switching to alternative banking providers. Aprilia and Amalia (2023) found that perceived security is a significant factor influencing customers' intention to continue using digital financial services, which implies that mitigating cyber-related risks is beneficial for customer retention. The Expectation Confirmation Model (ECM) also assists in understanding customer behaviour in digital banking. This model assumes that customers will continue using a service if they have satisfactory experiences, perceived usefulness, trust and reliable performance that meet their expectations. However, if service expectations are not met, customers will be dissatisfied and may look for other service providers. Lee et al. (2023) applied the ECM to AI-enabled mobile banking and reported that trust and system quality have a significant effect on continuance intention. Likewise, trust and perceived system quality still significantly predict customers' continued use of mobile banking (Nguyen & Dao, 2024; Saibaba, 2024). The ECM is a useful framework for explaining why poor cybersecurity may lead customers to switch from their current bank, as switching intention is the opposite of continuance intention.

2.2 Empirical Review

2.2.1. Perceived Security and Customer Switching Intention

Perceived security is known to be one of the most powerful factors impacting the behavior of customers in digital banking. Perceived security means the trust of customers in the ability of the bank to provide proper protection of their transactions and personal data from cyber threats. As a result, the customers are likely to be loyal to their banks and continue using the digital services.

According to Merhi et al. (2019), security and privacy are some of the key drivers for the adoption and continuous usage of mobile banking services. In addition, Aprilia and Amalia (2023) have identified that perceived security increases the customers' willingness to continue using digital financial services. Moreover, Panditharathna et al. (2024) demonstrated that cybersecurity makes a positive contribution to trust and commitment and improves customer retention as a result. Within the Nepalese context, the research works conducted by Adhikari (2024), Adhikari (2025), Amgain and Koirala (2025), and Regmi and Sah (2025) indicated that high security and reliability of electronic banking services leads to higher customer satisfaction and service quality. Even though none of these works studied the customers' switching intention, they all demonstrate the impact of perceived security on the decision-making process.

H1: *Perceived security has a significant negative effect on customer switching intention.*

2.2.2. Data Privacy and Customer Switching Intention

Data privacy is the level of confidence that financial institutions have in the secure collection, storage and use of customers' personal and financial information. As digital banking increasingly relies on electronic data exchange, protecting customer information is a critical part of cybersecurity.

Merhi et al. (2019) pointed out the importance of privacy protection among the factors affecting customers' willingness to use mobile banking services. Similarly, Panditharathna et al. (2024) showed that good data protection leads to higher customer trust and commitment. Furthermore, Tran (2025) emphasized the importance of robust data governance and privacy regulations in the context of contemporary banking cybersecurity. Goet and Kharel (2022), Thapa (2023), Bohara (2024), and Timalsina (2024) discovered that dependable and safe digital banking services enhance customer satisfaction and trust in Nepal. The results show that customers are more likely to continue to use banking services if they believe their personal information is well protected.

H2: *Data privacy has a significant negative effect on customer switching intention.*

2.2.3. Cyberattack experience and Customer Switching Intention

Customers who have experienced cyber incidents like phishing attacks, online fraud, unauthorized transactions or identity theft, are generally more cautious when it comes to using digital banking services. These experiences can result in a lower level of trust, higher perceived risk and influence future banking decisions.

Although the experience of cyberattack has seldom been included as an independent variable in previous studies, the existing evidence shows that security failures negatively affect customer confidence. As mentioned by Panditharathna et al. (2024), better cybersecurity leads to increased customer retention due to increased trust and commitment. Tran (2025) noted that cyber threats remain serious challenges for financial institutions globally. In addition, Nguyen and Dao (2024) and Saibaba (2024) concluded that trust and system quality have a significant effect on customers' intentions to continue using mobile banking. Cyberattacks often lead to loss of customer trust, and the quality of the system is felt to be reduced, which makes customers prone to look for alternative banking providers.

H3: Cyberattack experience has a significant and negative effect on customer switching intention.

2.2.4. Trust in the Bank's Security System and Customer Switching Intention Customer Switching Intention.

Confidence in the security system of a bank is when its clients believe that the bank's security system will protect their financial assets and online transactions. With high trust, perceived uncertainty is minimized and relationships with customers are strengthened in the long run.

According to Panditharathna et al. (2024), cybersecurity increases customer trust and commitment, which positively affect customer retention. Similarly, Merhi et al. (2019) found that trust, security and privacy are important factors for customer's intention to use mobile banking. Nguyen and Dao (2024) also found that trust is an important factor to enhance continuance intention and Lee et al. (2023) reported similar results for AI-enabled mobile banking applications. In Nepal, Bhatt and Nepali (2021) and Karmacharya (2024) noted that trust remains one of the strongest determinants of customer loyalty and relationship quality in commercial banking. The results, taken together, suggest that customers who trust the security system of their bank are less likely to switch to competing banks.

H4: Trust in the bank's security system has a significant postive effect on customer switching intention.

2.2.5. Cybersecurity Awareness and Customer Switching Intention

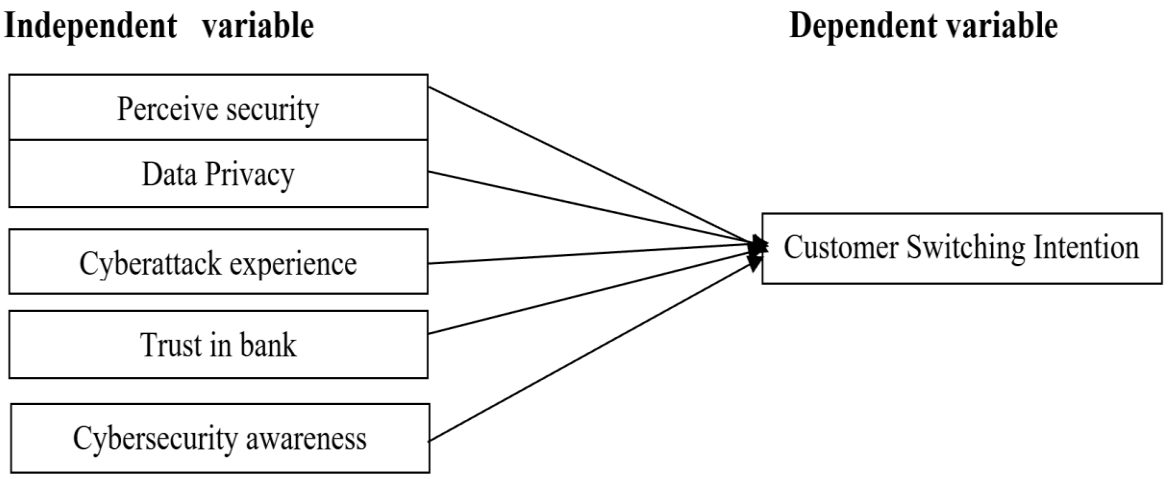
Cybersecurity awareness is defined as the awareness of customers regarding cyber threats, online fraud, password protection, phishing attack and secure digital banking practices. Higher awareness among customers generally allows them to better assess the security of digital banking platforms and identify potential risks.

Effective cybersecurity is not only dependent on technological infrastructure but also on users' awareness and understanding of digital security practices, said Tran (2025). Similarly, Panditharathna et al. (2024) argued that customers' awareness influences their evaluation of the banks' cybersecurity measures. Shaikh and Karjaluoto (2015) also stated that customers' perceptions of security and risk are highly related to customers' knowledge of digital banking. Studies from Nepal by Bohara (2024), Goet and Kharel (2022) and Thapa (2023) showed that as digital banking is growing, cybersecurity awareness is becoming more and more important for customers. Thus, the increased awareness can affect customers' choices to stay or change banks, depending on their perceptions of the effectiveness of their bank's cybersecurity practices.

H5: Cybersecurity awareness has a significant positive effect on customer switching intention.

2.3 Conceptual framework

Figure 1. *Conceptual framework*



Note: Adpated from Panditharathna et al., 2024; Rahi et al., 2020; Sharma & Sharma, 2019; Alalwan et al., 2018)

3. RESEARCH METHODOLOGY

3.1 Research Design

The study used a quantitative, cross-sectional design to examine associations between cybersecurity-related perceptions and customer switching intention. Data were collected at one point in time. The design can identify associations but cannot establish cause-and-effect relationships or changes over time.

3.2 Population, Sample Size, and Sampling Technique

The target population comprised customers of commercial banks in Rupandehi District, Nepal. Since the exact number of banking customers is unknown, Cochran's (1977) formula for an infinite population was used to determine the sample size.

$$n_o = \frac{Z^2 * p * q}{e^2}$$

Where:

n_0 = required sample size
Z = z-value at 95% confidence level (1.96)
p = estimated proportion (0.5)
q = 1 − p (0.5)
e = margin of error (0.05)

The study collected data from 297 banking customers, below the stated recommended sample size of 384. Participants were recruited through convenience sampling, which may introduce selection bias and limits representativeness. Please report how the target of 384 was calculated, numbers distributed and returned, eligibility criteria, and any exclusions. Consider these limitations when interpreting the results.

3.3 Nature and Sources of Data

The research used primary quantitative data gathered from the banking customers themselves. Primary data were deemed suitable for the research since they gave information about the customer perceptions about cybersecurity and switching intentions.

3.4 Data Collection Instrument

Data were collected using a structured questionnaire developed from validated scales used in previous studies. The questionnaire consisted of 30 items measuring perceived security, data privacy, cyberattack experience, trust in the bank's security system, cybersecurity awareness, and customer switching intention. All items were measured using a seven-point Likert scale, ranging from 1 (Strongly Disagree) to 7 (Strongly Agree).

Item for Perceived Security were adapted from Panditharathna et al. (2024) and Rahi et al. (2020) and Alalwan et al. (2018).Data Privacy were adapted from Panditharathna et al. (2024) and Sharma & Sharma (2019) and Tran (2025).Cyberattack Experience were adapted from Bhatt & Nepali (2021) and NRB cyber risk context and Panditharathna et al. (2024),Trust in Bank's Security System were adapted from Panditharathna et al. (2024) and Rahi et al. (2020) and Sharma & Sharma (2019).Cybersecurity Awareness were adapted from Bhatt & Nepali (2021) and Tran (2025) and Panditharathna et al. (2024).Customer Switching Intention were adapted from Panditharathna et al. (2024) and Sharma & Sharma (2019) and Rahi et al. (2020)

3.5 Data Analysis Techniques

The collected data were analyzed using SPSS 20 and SmartPLS software. Descriptive statistics were used to summarize respondents' characteristics and variable distributions. The measurement model was evaluated using reliability and validity tests, including Cronbach's alpha, composite reliability, average variance extracted (AVE), HTMT, and the Fornell–Larcker criterion. Common Method Bias (CMB) was assessed using Harman's single-factor test. The structural model was then analyzed using Partial Least Squares Structural Equation Modelling (PLS-SEM) to test the proposed hypotheses. In addition, Importance–Performance Map Analysis (IPMA) and Necessary Condition Analysis (NCA) were performed to identify the relative importance and necessary conditions of the independent variables influencing customer switching intention.

4. RESULT AND ANALYSIS

4.1 Respondent's Profile

Table 1 - *Descriptive statistics of participant*

Gender	**F**	**%**	**Occupation**	**f**	**%**
Male	166	55.9	Student	110	37.0
Female	131	44.1	Employee	113	38.0
			Business	62	20.9
Age	**F**	**%**	Other	12	4.0
Below 25	139	46.8			
25–34	100	33.7	**Type of Bank Used**	**f**	**%**
35–44	44	14.8	Public Bank	97	32.7
45 and above	14	4.7	Private Bank	141	47.5
			Both	59	19.9
Education Level	**F**	**%**			
+2 and below	64	21.5	**Years of Banking Experience**	**f**	**%**
Bachelor's	147	49.5	Below 2 years	95	32.0
Master's	71	23.9	2–5 years	120	40.4
Above Master's	15	5.1	6–10 years	58	19.5
			Above 10 years	24	8.1
Use of Digital Banking Services	**F**	**%**			
Yes	251	84.5			
No	46	15.5			

Table presents the demographic characteristics and banking behavior of the respondents. It shows that most of the respondents are male (55.9%) and females are 44.1% that shows a little bit higher male participation. The majority of the respondents are young. 46.8% are below 25 years and 33.7% are in the age group of 25-34 years. Only a small percentage is in the older age groups. The highest level of education among respondents is Bachelor's degree for almost half of the respondents (49.5%) and Master's degree for 23.9% of respondents, indicating a mostly well-educated sample. The most numerous groups according to the occupation are employees (38.0%) and students (37.0%). Less respondents are engaged in business (20.9%) and other activities (4.0%). The data also reveals that private banks are used more often (47.5%) than public banks (32.7%) and 19.9% of respondents use both types. In terms of banking experience, most of them have 2–5 years' experience (40.4%), followed by those with less than 2 years (32.0%), indicating relatively moderate experience levels. Finally, a large proportion of respondents (84.5%) use digital banking services with only 15.5% not using digital banking services, indicating a high level of adoption of digital banking. The results indicate that the respondents are mostly young, well-educated people who prefer private banks and are active users of digital banking services.

4.2 Common Method Bias (CMB)

Table 2 - *Variance Explained*

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	13.758	45.861	45.861	13.758	45.861	45.861
2	4.341	14.471	60.333			
3	1.991	6.636	66.969			
4	1.347	4.490	71.459			
5	1.025	3.415	74.874			
6	.770	2.567	77.441			
7	.703	2.342	79.783			
8	.642	2.139	81.921			
9	.567	1.889	83.811			
10	.504	1.680	85.490			
11	.448	1.495	86.985			
12	.431	1.435	88.420			
13	.403	1.344	89.765			
14	.363	1.209	90.974			
15	.346	1.154	92.128			
16	.320	1.068	93.196			
17	.311	1.037	94.233			
18	.267	.889	95.122			
19	.241	.804	95.926			
20	.213	.709	96.635			
21	.190	.633	97.267			
22	.180	.599	97.866			
23	.164	.547	98.414			
24	.152	.508	98.922			
25	.131	.436	99.358			
26	.104	.347	99.706			
27	.088	.294	100.000			
28	1.24	4.13	100.000			
29	-8.9	-2.98	100.000			
30	-2.4	-8.00	100.000			

A

Harman single-factor analysis using principal component analysis is reported in Table 2. The first factor accounts for 45.861% of the variance, below the 50% rule of thumb cited in the manuscript. This result alone does not establish that common method bias is absent or prove the validity of the empirical evidence. Please verify the table against the original SPSS output: rows for components 28-30 contain malformed eigenvalue and variance entries. Clarify the extraction and rotation settings and report any procedural safeguards or additional diagnostics.

4.3 Measurement Item Assessment

Table 3 - *Assessment of scale item*

Name	Outer loadings	VIF	Mean	Standard deviation
Q1	0.869	2.898	5.946	1.394
Q2	0.911	4.036	5.808	1.498

Q3	0.917	4.297	5.7	1.654
Q4	0.745	1.857	5.013	1.775
Q5	0.765	1.715	5.495	1.706
Q6	0.749	1.813	4.694	1.808
Q7	0.81	2.605	5.104	1.511
Q8	0.826	2.481	5.114	1.694
Q9	0.862	3.88	5.899	1.487
Q10	0.776	3.148	6.219	1.359
Q11	0.9	3.176	3.276	1.881
Q12	0.882	3.111	3.657	1.981
Q13	0.838	2.392	3.613	2.065
Q14	0.819	2.316	4.101	1.957
Q15	0.919	4.236	3.781	1.965
Q16	0.826	2.68	3.599	1.94
Q17	0.838	2.978	3.138	1.862
Q18	0.922	4.051	3.744	1.886
Q19	0.894	3.531	3.785	1.961
Q20	0.793	1.912	4.724	1.881
Q21	0.711	1.445	5.162	1.714
Q22	0.889	3.231	5.118	1.551
Q23	0.797	2.208	4.694	1.808
Q24	0.865	2.639	5.104	1.511
Q25	0.695	1.48	4.828	1.781
Q26	0.794	1.871	5.542	1.546
Q27	0.813	2.363	5.714	1.507
Q28	0.881	3.052	5.576	1.54
Q29	0.866	3.636	4.929	1.744
Q30	0.777	2.675	4.576	1.734

Table 3 reports outer loadings, VIFs, means, and standard deviations. The listed loadings range from 0.695 to 0.922; Q25 is the only item below 0.70 (0.695). Please state whether Q25 was retained or removed from the final model and explain the decision using construct-level AVE, reliability, and content validity. Item VIF values below 5 do not prove that multicollinearity is absent under all criteria.

4.4: Quality Criteria Assessment

Table 4 - *Construct reliability and validity*

Variable	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Customer Switching Intention	0.884	0.888	0.915	0.684
Cyberattack Experience	0.921	0.933	0.941	0.761
Cybersecurity Awareness	0.851	0.860	0.895	0.633
Data Privacy	0.864	0.870	0.902	0.649
Perceived Security	0.897	0.903	0.925	0.713
Trust in Bank's Security System	0.909	0.922	0.932	0.732

Table 4 reports Cronbach's alpha values from 0.851 to 0.921, composite reliability values from 0.860 to 0.941, and AVE values from 0.633 to 0.761. These values meet the thresholds stated in

the manuscript, supporting internal consistency and convergent validity under those criteria. AVE is a construct-level statistic and should not be described as showing that each indicator individually explains more than 50% of variance.

Table 5 - *Heterotrait Monotrait (HTMT) ratio of correlation*

	Customer Switching Intention	Cyberattack Experience	Cybersecurity Awareness	Data Privacy	Perceived Security	Trust in Bank's Security System
Customer Switching Intention						
Cyberattack Experience	0.456					
Cybersecurity Awareness	0.881	0.420				
Data Privacy	0.676	0.492	0.834			
Perceived Security	0.895	0.537	0.742	0.831		
Trust in Bank's Security System	0.465	0.890	0.425	0.462	0.474	

Table 5 reports HTMT values from 0.420 to 0.895. Three values exceed the stricter 0.85 criterion: customer switching intention with cybersecurity awareness (0.881), customer switching intention with perceived security (0.895), and cyberattack experience with trust in the bank's security system (0.890). All listed values are below 0.90, but the discriminant-validity conclusion depends on the criterion adopted. HTMT assesses discriminant validity, not multicollinearity. State the prespecified threshold and report bootstrap confidence intervals if available.

Table 6 - *Fornell- Larcker Criterion*

	Customer Switching Intention	Cyberattack Experience	Cybersecurity Awareness	Data Privacy	Perceived Security	Trust in Bank's Security System
Customer Switching Intention	**0.827**					
Cyberattack Experience	-0.421	**0.872**				
Cybersecurity Awareness	0.767	-0.380	**0.795**			
Data Privacy	0.728	-0.445	0.602	**0.805**		
Perceived Security	0.803	-0.498	0.647	0.738	**0.844**	
Trust in Bank's Security System	0.432	-0.835	0.388	0.425	0.445	**0.856**

In Table 6, each diagonal square-root-of-AVE value is greater than the absolute value of the corresponding off-diagonal construct correlations, consistent with the Fornell-Larcker criterion. This evidence should be considered alongside the HTMT results in Table 5, which include three values above 0.85. Neither criterion establishes the absence of multicollinearity.

4.5 Model Fit indices

Table 7 - *Model Fit*

	Saturated model	**Estimated model**
SRMR	0.076	0.076
d_ULS	1.400	1.400
d_G	0.578	0.578
Chi-square	1067.78	1067.78
NFI	0.886	0.886

Table 7 reports SRMR = 0.076 and NFI = 0.886 for both the saturated and estimated models. The SRMR is below the 0.08 reference cited in the manuscript, whereas the NFI is below 0.90. The original narrative incorrectly states that 0.886 exceeds 0.90 and repeats the same interpretation. Report these indices accurately and interpret fit cautiously; SRMR and NFI do not establish explanatory or predictive power.

Table 8 - *f- Square (effect size)*

	f-square	Effect Size
Cyberattack Experience -> Customer Switching Intention	0.019	No effect
Cybersecurity Awareness -> Customer Switching Intention	0.014	No effect
Data Privacy -> Customer Switching Intention	0.098	Small
Perceived Security -> Customer Switching Intention	0.358	Large
Trust in Bank's Security System -> Customer Switching Intention	0.020	Small

Table 8 reports f-squared values of 0.019 for cyberattack experience and 0.014 for cybersecurity awareness (negligible under the conventional 0.02 reference), 0.098 for data privacy (small), 0.358 for perceived security (large), and 0.020 for trust in the bank's security system (small at the conventional lower boundary). The table's classification of data privacy as a large effect is inconsistent with its value and should be corrected.

Table 9 - *R – square*

	R-square	**R-square adjusted**	**Predictive power**
Customer Switching Intention	0.776	0.772	Substantial

Table 9 reports R-squared = 0.776 and adjusted R-squared = 0.772 for customer switching intention. The model therefore accounts for 77.6% of sample variance in the outcome (adjusted estimate: 77.2%). This statistic describes in-sample explanatory power; it does not by itself establish predictive capability or generalisability.

Figure 2: SEM Model

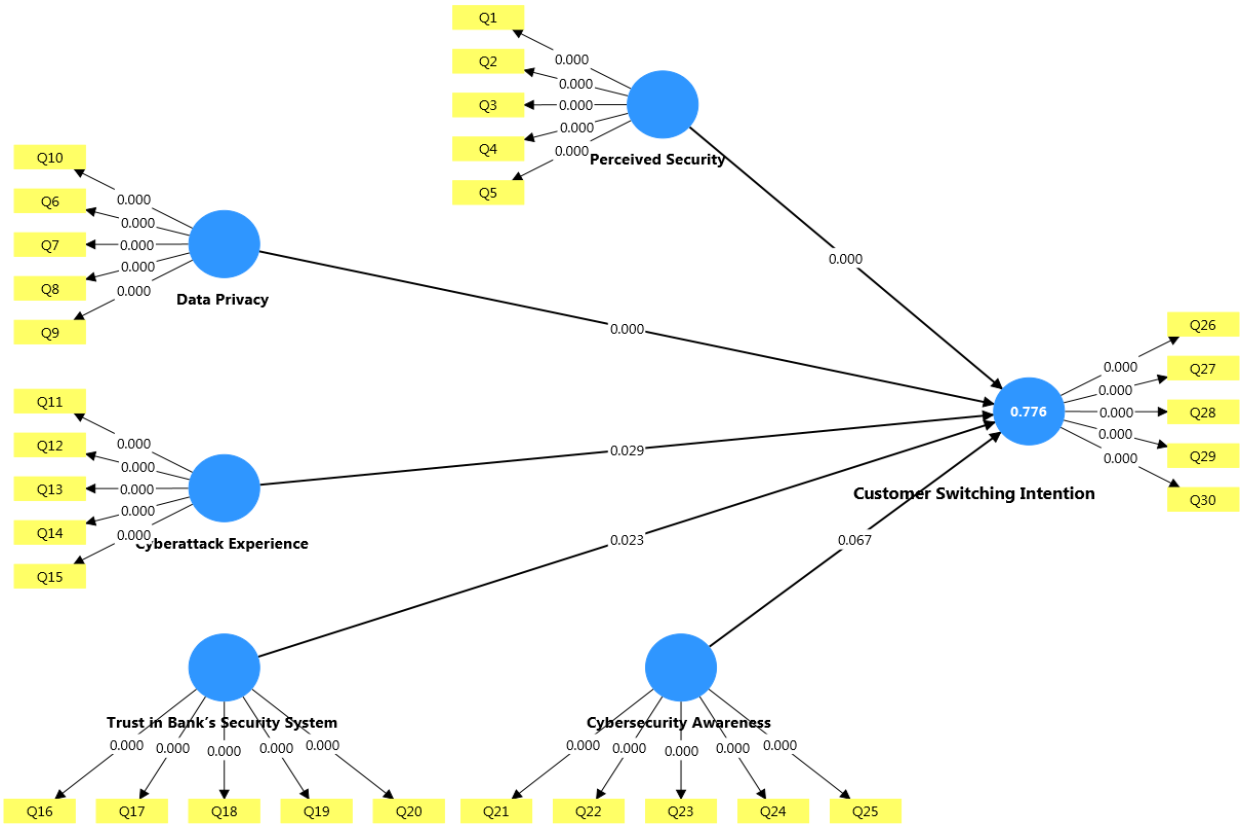


Table 10 - *Hypothesis testing using bootstrapping*

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values	Decision
H1: Perceived Security -> Customer Switching Intention	-0.438	0.442	0.063	6.899	0.000	<0.001
H2: Data Privacy -> Customer Switching Intention	-0.390	0.389	0.087	4.481	0.000	<0.001
H3: Cyberattack Experience -> Customer Switching Intention	-0.123	0.124	0.056	2.189	0.029	Supported
H4: Trust in Bank's Security System -> Customer Switching Intention	-0.123	0.123	0.054	2.269	0.023	supported
H5: Cybersecurity Awareness -> Customer Switching Intention	0.131	0.127	0.071	1.832	0.067	Not supported

Table 10 reports statistically significant negative path coefficients for perceived security (beta = -0.438, p below 0.001), data privacy (beta = -0.390, p below 0.001), cyberattack experience (beta = -0.123, p = 0.029), and trust in the bank's security system (beta = -0.123, p = 0.023). Cybersecurity awareness has a positive but nonsignificant coefficient (beta = 0.131, p = 0.067). The narrative must reflect these directions, not describe the significant negative coefficients as positive effects. The cyberattack-experience result is contrary to the stated theoretical expectation and warrants verification of coding and output.

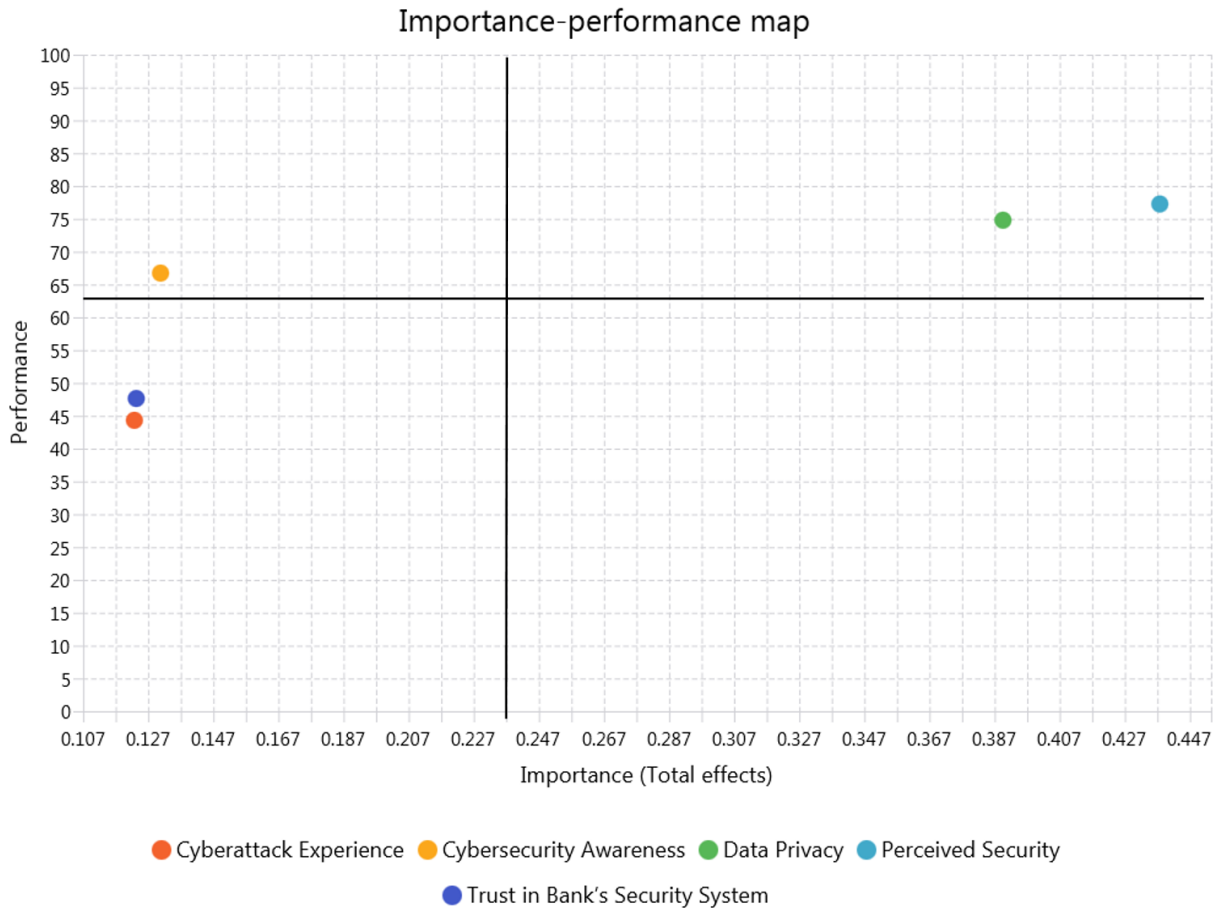
4.7 **Importance performance map analysis (IPMA)**

Table 11 - *Information performance map analysis*

	LV performance	**Importance**
Cyberattack Experience	44.318	0.123
Cybersecurity Awareness	66.739	0.131
Data Privacy	74.797	0.39
Perceived Security	77.266	0.438
Trust in Bank's Security System	47.638	0.123
Mean	62.1516	0.241

Table 11 reports perceived security as having the highest importance (0.438), followed by data privacy (0.390), cybersecurity awareness (0.131), cyberattack experience (0.123), and trust in the bank's security system (0.123). The performance value for perceived security is 77.266. The table does not report the stated projected increase in switching-intention performance from 72.008 to 72.466. Verify the calculation against the original IPMA output or remove the projection. IPMA importance should not be described as an effect size.

Figure 3 - *Importance Performance Map*



4.8 Necessary Condition Analysis (NCA)

Table 12 - *Bottleneck Percentile*

Customer Switching Intention	LV scores - Cyberattack Experience	LV scores - Cybersecurity Awareness	LV scores - Data Privacy	LV scores - Perceived Security	LV scores - Trust in Bank's Security System
0.000%	NN	NN	NN	NN	NN
10.000%	NN	2.69%	NN	NN	NN
20.000%	NN	3.70%	5.38%	NN	NN
30.000%	NN	3.70%	7.74%	5.72%	NN
40.000%	NN	3.70%	7.74%	5.72%	NN
50.000%	NN	3.70%	7.74%	5.72%	NN
60.000%	NN	3.70%	7.74%	5.72%	NN
70.000%	NN	5.38%	7.74%	5.72%	NN
80.000%	NN	9.42%	14.14%	5.72%	NN
90.000%	NN	24.24%	31.31%	5.72%	NN
100.000%	NN	61.95%	72.05%	5.72%	2.02 %

Table 12 reports NCA bottleneck levels. At a 10% switching-intention target, cybersecurity awareness is listed at 2.69%, while the other constructs are marked NN. At 20%, awareness is 3.70% and data privacy is 5.38%; at 80%, awareness is 9.42%, data privacy is 14.14%, and perceived security is 5.72%. At 100%, awareness is 61.95%, data privacy is 72.05%, perceived security is 5.72%, and trust is 2.02%; cyberattack experience is marked NN. These are bottleneck levels, not causal effects. Define NN and the scale/units and verify the NCA output before drawing substantive conclusions.

5. DISCUSSION

This study examined associations between cybersecurity-related perceptions and customer switching intention among banking customers in Rupandehi District. The model explained 77.6%

of sample variance. Table 10 reports statistically significant negative path coefficients for perceived security, data privacy, cyberattack experience, and trust; cybersecurity awareness had a positive but nonsignificant coefficient. These signs should be verified against construct coding and the original output, especially for cyberattack experience. Given the cross-sectional convenience sample, the results are associational and may not generalize beyond respondents.

The study also found that data privacy has a huge effect on customer switching intention. Customers have higher expectations that banks will safeguard their personal and financial information from being accessed and used without permission. The protection of customer data has become vital for retention of trust and reduction of switching behaviour with the continued expansion of digital banking services. This result is in line with previous studies by Merhi et al. (2019) and Tran (2025), highlighting the significance of robust data privacy and governance in building customer trust and cultivating lasting relationships with financial institutions.

Moreover, the experience of cyberattack was found to have a significant effect on the switching intention of the customer. Customers that have experienced or been exposed to cyber incidents tend to be more cautious when assessing the security of banking services. These experiences raise the perceived risk and lower the confidence in the platforms of digital banking, making the customers more prone to look at alternative banking providers. This finding aligns with Panditharathna et al. (2024) and Tran (2025) who indicate that cybersecurity incidents negatively impact customer trust and emphasize the importance of effective cyber risk management in the banking sector.

The results also show that customer trust in the bank's security system has a significant effect on customer switching intention. Those who believe in the security of their bank's cyber infrastructure are more confident in conducting their business digitally and less likely to switch to a competing bank. Trust is an important part of long-term relationships with customers because it reduces uncertainty and increases perceptions of reliability among customers. This finding is consistent with Merhi et al. (2019), Nguyen and Dao (2024), and Lee et al. (2023), who found that trust is a key factor in customers' continuous use of digital banking services.

On the other hand, cybersecurity awareness was not statistically significant in influencing customer intention to switch. Customers may have knowledge of the cyber threats and online security practices, but knowledge does not seem to have an impact on the customer's decision to stay or leave a bank. Instead, customers are more swayed by the real security measures financial institutions put in place. This result shows that simply increasing customer awareness is not enough to reduce switching behavior unless banks also show that they have strong security systems and are effective in protecting customer information.

In general, results support the Theory of Planned Behavior and the Relationship Quality Theory, suggesting that behavioural intentions are influenced by customers' perceptions, trust and evaluations of service quality. In the era of digital banking , customers tend to develop long-term relationships with banks that offer secure digital platforms , secure customer data and build trust through good cyber security practices . As digital financial services continue to evolve in Nepal, commercial banks may consider strengthening cybersecurity as a strategic priority to enhance customer confidence and reduce switching behavior.

6.CONCLUSION AND IMPLICATION

6.1 Conclusion

The study examined the impact of cybersecurity on the customer's switching intention in the banking sector of Rupandehi District, Nepal. The results show that cybersecurity has a significant influence on customers' decisions to stay or leave their bank. Among the factors examined, perceived security emerged as the strongest predictor of customer switching intention, followed by data privacy, cyberattack experience, and trust in the bank's security system. In contrast, cybersecurity awareness had no significant effect, suggesting that customers are more concerned with the actual security measures taken by banks than their own level of cybersecurity awareness.

The present study adds to the literature by extending the cybersecurity research from customer satisfaction and continuance intention to customer switching intention in the Nepalese banking industry. The findings highlight the importance of improving cybersecurity practices to improve customer trust and protect sensitive information and curtail customer switching behaviour. Digital banking is on the rise in Nepal and investing in robust cybersecurity will be a must to build up customer confidence and develop long-term customer relationships in banking industry.

6.2 Implications

This study adds to the literature of cybersecurity by focusing on its effect on customers' switching intention, which is rarely addressed in the previous studies. Previous studies focus on customer satisfaction, loyalty and continuance intention. This study reveals that perceived security, data privacy, cyberattack experience and trust in the security system of the bank are significant determinants of customers' switching behavior. The results also support the Theory of Planned Behaviour and Relationship Quality Theory and highlight the importance of security, trust and privacy in influencing customers' behavioural intentions in digital banking.

The findings offer useful insights to commercial banks and policy makers. Banks need to invest in advanced security technologies, multi-factor authentication, fraud detection systems and robust data protection measures to strengthen cybersecurity and improve customer trust and reduce switching behaviour. Greater clarity around cybersecurity policies and educating customers about digital security practices can further boost confidence in digital banking services. Furthermore, Nepal Rastra Bank and other regulatory bodies should continue developing and enforcing comprehensive cybersecurity standards and data protection policies to guarantee a secure digital banking environment and boost customer confidence in Nepal's financial sector**.**

7. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

7.1 Limitation

This study has several limitations. It was conducted among customers in Rupandehi District, used convenience sampling, and measured perceptions at one point in time; these features limit representativeness, causal interpretation, and generalisability. The self-reported questionnaire may be subject to response and common-method biases. The study focused on five cybersecurity-related constructs and did not include other potential determinants of switching intention. Future research could use probability sampling, longitudinal or mixed-source data, broader samples, and validated measures.

7.2 Future Research Directions

Future research should include respondents from different districts or provinces of Nepal to improve the generalizability of the results. Longitudinal studies are required to study the evolution of customer perceptions of cybersecurity and switching intentions over time. Probability sampling techniques can be used by future researchers to obtain more representative samples and enhance external validity of the results. To build a more comprehensive model, other variables could be added, such as perceived risk, customer satisfaction, customer loyalty, service quality, digital literacy, switching cost, and technology readiness. Further studies could examine the mediating or moderating effects of variables such as trust, perceived risk, customer satisfaction, age, gender or digital banking experience for further insights into customer switching behavior.

8. REFERENCE

- Adhikari, N. B. (2024). Impact of Electronic Banking on Customer Satisfaction in Nepalese Commercial Banks. *Kalika Journal of Multidisciplinary Studies*, *6*(1), 66-77.
- Adhikari, S. R. (2025). E-Banking Services and Customer Satisfaction of Nepalese Commercial Banks. *The Mega Journal*, *4*(1), 10-24.
- Alalwan, A., Dwivedi, Y., & Williams, M. (2014). Examining factors affecting customer intention and adoption of internet banking in Jordan.
- Alawneh, A. A. (2013). Assessing the dimensions of relationship quality in B2C e banking services: An empirical comparative study. *arXiv preprint arXiv:1302.6364*.
- Amgain, P. N., & Koirala, N. (2025). Investigating Electronic Banking Services on Customer Satisfaction in Commercial Banks. *Victoria Journal of Management*, *2*(2), 127-148.
- Aprilia, C., & Amalia, R. (2023). Perceived security and technology continuance theory: An analysis of mobile wallet users' continuance intention. *Global Business Review*, 09721509221145831.
- Bhatt, S., & Nepali, N. K. (2021). Factors affecting Customer Loyalty (A study of banking customers in Rupandehi District). *Bhairahawa Campus Journal*, 1-8.
- Bland, J. M., & Altman, D. G. (1997). Statistics notes: Cronbach's alpha. *Bmj*, *314*(7080), 572.
- Bohara, Y. (2024). Factors affecting customer satisfaction of mobile banking in Nepalese commercial banks. *Nepalese Journal of Management*, *11*(2), 208-227.
- Cochran, W. G. (1977). *Sampling techniques*. john wiley & sons.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.
- Goet, J., & Kharel, K. (2022). Customer satisfaction with mobile banking services in Nepalese commercial banks. *Management Dynamics*, *25*(2), 23-30.
- Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research methods in applied linguistics*, *1*(3), 100027.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, *43*(1), 115-135.
- Hu, L. T., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological methods*, *3*(4), 424.
- Karmacharya, B. (2025). Examining the Role of e-CRM in Boosting Customer Satisfaction in Financial Institutions in Nepal: A Two-Stage PLS-SEM and ANN Approach. *Prithvi Academic Journal*, *8*, 47-64.
- Lee, J. C., Tang, Y., & Jiang, S. (2023). Understanding continuance intention of artificial intelligence (AI)-enabled mobile banking applications: an extension of AI characteristics to an expectation confirmation model. *Humanities and Social Sciences Communications*, *10*(1), 333.
- 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*, *59*, 101151.
- Nguyen, G. D., & Dao, T. H. T. (2024). Factors influencing continuance intention to use mobile banking: an extended expectation-confirmation model with moderating role of trust. *Humanities and Social Sciences Communications*, *11*(1), 1-14.
- Panditharathna, R., Liu, Y., de Macedo Bergamo, F. V., Appiah, D., Trim, P. R., & Lee, Y. I. (2024). How cyber security enhances trust and commitment to customer retention: the mediating role of robotic service quality. *Big Data and Cognitive Computing*, *8*(11), 165.

- Rahi, S., Ghani, M. A., & Ngah, A. H. (2020). Factors propelling the adoption of internet banking: the role of e-customer service, website design, brand image and customer satisfaction. *International Journal of Business Information Systems*, *33*(4), 549-569.
- Saibaba, S. (2024). Examining the determinants of mobile banking app continuance intention in India: An extension of the IS success model. *Journal of Internet Commerce*, *23*(1), 50-89.
- Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In *Handbook of market research* (pp. 587-632). Cham: Springer International Publishing.
- Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and informatics*, *32*(1), 129-142.
- 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.
- Thapa, M. (2023). E-banking services and customer satisfaction with reference to Nepalese banking sector. *Journal of Business and Social Sciences*, *5*(1), 55-68.
- Timalsina, D. (2024). Determinants of Customer Satisfaction on Retail Banking in Nepal. *Bhairahawa Campus Journal*, *7*(1), 15-26.
- Tran, T. N. (2025). Systematic Review of Cybersecurity in Banking: Evolution from Pre-Industry 4.0 to Post-Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice. *arXiv preprint arXiv:2503.0007*
- 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.