Innovations

Adoption of Online Banking Security Measures by customers – Evaluation through Extended Technology Acceptance Model (TAM) and Structural Equation Model (SEM)

Dr Gopu Jayaraman *
Dr.V. Mahalakshmi Venkatachalam**
Dr Hanaa Mahmoud Sid Ahmed*
Dr Muawya Ahmed Hussien***

*Assistant Professor, Business Administration, the University of Technology and Applied Sciences, (CEBA), Salalah, Sultanate of Oman (Corresponding Author)
** Assistant Professor, Department of Computer Science & Engineering, FEAT, Annamalai University, India
***Assistant Professor, Dhofar University, Salalah, Sultanate of Oman
Corresponding Author: Dr Gopu Jayaraman

Abstract

Objectives – *In light ofthe introduction of online banking services, the purpose of this paper is to evaluate the adoption of online banking security measures by customers.* ***Methodology–*** *The paperhas adopted the quantitative research design with a link to the deductive method by investigating existing literature, and theories and developing hypotheses, conducting surveys and testing the hypotheses through the Extended Technology Acceptance Model (Extended TAM). The impact of customers' frequency of online banking, perceived usage and ease of using online security measures and perceived risk of not adopting security measures on the intention of adopting security measures are investigated and the impact is measured via the mediator (Attitude). The analysis was done using the powerful statistical technique of the Partial Least Square - Structural equation model (PLS-SEM), and the WarpPLS Software 8.00 Version (Latest) was applied to test the model.* ***Results-*** *The frequency of online banking and perceived risk have direct as well as indirect effects (through Attitude) on the customer's intention to adopt security measures, whereas the perceived use and usage of security measures have an indirect effect on the customers' attitude. The direct path effects of perceived use and ease of using security measures to intention are not statistically significant but the indirect effect through mediation is statistically significant.* ***Practical implications-*** *This study brought out significant conceptual clarity about customers' behaviour in using online banking security measures. This study has important theoretical contributions and implications as there are not many previous studies focused on online banking security measures. The discussions and results of this research work will immensely be useful to commercial banks in understanding the customers' adoption process of online banking security measures. The study can be useful for further research in the areas of online banking security measures.* ***Originality value****-The paper offers a new analysis of existing sources on e-banking and provides new visions into the topic area by emphasizing its relationship with collaborative working using many tests. This research adequately investigated online banking security measures and represents a substantial contribution to the literature, especially in the lack of adequate literature about online banking security measures.*

Keywords: 1.*Online banking, 2.Online banking security measures, 3.Perceived use, 4.Perceived ease of use, 5.Extended technology acceptance model, 6.Structural equation model, 7.perceived risk, 8.Adoption of security measures.*

1. Introduction

The rapid developments and innovations in Information technology redefined the way of doing various business sector, especially the financial services sector, Khan, Hameed, and Khan (2017) digital devices has

spotlighted the wisdom of doing financial transactions through online banking. The advancement of technology and speedy growth of internet users facilitate and motivate people to go for online transactionsKabir and Islam (2021); (Singh & Srivastava, 2020)**.** The banking transactions and services offered by banks and availed by the customers are called Online banking, Musaev and Yousoof (2015)several other terms such as e-banking, internet banking, mobile banking,etc. are used to represent online banking.Onlinebanking provides a lot of benefits but is subject to a series of risks,Khan et al. (2017)security is the major issue of online banking, andAribake (2015)observed that maintaining security is a challenge for banks.A simple security slip on the customer may result in the account details goinginto the wrong hands and potentially emptyingthe customer's account from anywhere in the world. Cybercriminalssteal account details and credentials through various methods, such as Phishing Olalere, Waziri, Ismaila, and Ololade (2014)**,** Malwares Jansen and Leukfeldt (2016)**,** Pharming and Trojan horseJansen and Leukfeldt (2016)**,**

The banks should understand how their customers perceive and adopt the security measures implemented for onlinebanking servicesMusaev and Yousoof (2015)**,** the secured online banking experience will certainly induce customers to increase their usage**,**de Oliveira Santini, Ladeira, Sampaio, and Perin (2018)found that satisfaction with online banking services promotes trust and loyalty. Since the introduction of onlinebanking services, a significant number of research works were carried out to examinevarious issues concerningonlinebanking.Singh and Srivastava (2020), (Al-Fahim, 2012; Safari, Bisimwa, & Armel, 2020)&(Al-Ajam & Nor, 2015)**,** studied the factors affecting customers' intention toward the adoption of Internet banking services, Jansen and Leukfeldt (2016),Pakojwar and Uke (2014),Alghazo, Kazmi, and Latif (2017),Aribake (2015), Chandio, Irani, Zeki, Shah, and Shah (2017)**,** researched the issues relating to the securities of the onlinebanking system, Alalwan, Dwivedi, Rana, and Algharabat (2018)**,** Tarhini, El-Masri, Ali, and Serrano (2016), Tang, Lai, Law, Liew, and Phua (2014), Makanyeza and Mutambayashata (2018),Hu and Khanam (2016), Singh and Srivastava (2020)**,** Al-Fahim (2012)studied customers adoption of internet banking using UTAUT and TAM Models. The various research models such as UTAUT, TAM, and SEM adopted by researchers significantly contributed to the knowledge base and formed sound guidelines for the banking sector to improve their onlinebanking services further. However, there are hardly a few studies concerning the customers' adoption of security guidelines of online banking services, for example, the research works carried out by Pakojwar and Uke (2014),**Chen and Corriveau (2009),**Jansen and Leukfeldt (2016), andAlghazo et al. (2017)&Aribake (2015)**,**mainly focus on strengthening the security side of onlinebanking which are highly technical.There is a lack of research on the security aspects of internet banking services Salem, Baidoun, and Walsh (2019), especially, in the absence of adequate research works relating to security measures adopted by onlinebanking customers in Middle Eastern countries like Oman it becomes relevant and necessary to undertake research work in the above-mentioned topics.

Based on the foregoing discussions, the present research work has been undertaken with the following specific objectives;

a) To study the impact of customers'online bankingexperience on their attitude and adoption of security measures suggested by banks for safe and secured online banking in the Sultanate of Oman
b) To study the influence of customers' perceived usefulness of the security measureson their attitude towards onlinebanking security measures.
c) To study the effect of customers' perceived ease of using the security measures on their attitude and adoption of the security measures.
d) To study the influence of customers' perceived risk of online banking without adopting security measures on their attitude and adoption of the security measures.

This research paper presents a model which will certainly help bankers, regulatory authorities, and researchers to have a better understanding of only banking customer perceptions and behaviour towards adopting the security measures for safe and secured onlinebanking.

2. Theoretical background of the study and hypotheses development

The theoretical framework of this study is based on the Technological Acceptance Model (TAM) developed by Davis (1989). The Technology Acceptance Model (TAM) Model was introduced by Fred Davis in 1989 and since then TAM Model has been extensively used to predict the user's intention in adopting new technologies,Jiang et al. (2022) it is most suitable for research in the field of online banking. The TAM Model is

very effective to evaluate the factors behind the customer's intention to adopt new technologiesSingh and Srivastava (2020), AlKailani (2016), Vuković, Pivac, and Kundid (2019), Safari et al. (2020). The TAM Model evolved with major constructs of technology users' perceived usefulness, perceived ease of use, attitude, and intention to use the technology. However, the researchers subsequently extended the model by adding or modifying the constructs based on the development in the customer's adoption of new technologies. For example, AlKailani (2016) in their study added three constructs (bank credibility, perceived risk, and perceived trust) to the TAM Model, and Singh and Srivastava (2020) added self-efficacy and social influence as additional constructs, The researchers extended TAM Model with additional constructor finding accurate answers to the question of what motivates users to use Internet bankingVuković et al. (2019), Singh and Srivastava (2020), Safari et al. (2020).

2.1 Customers'experience and frequency of using (FRE) online banking services

The customers' experience in terms of the period and frequency of using online banking for various types of transactions (travel and hotel bookings, bill and fee payments, shopping, stock market and investment transactions, balance and other inquiries, fund transfers, and requests for cheque books and statements) will influence their attitude and intention toward adopting online banking security measures.Polasik and Wisniewski (2009), stated that many researchers have included customers'experience of online banking in their research model, Giovanis, Binioris, and Polychronopoulos (2012), the experience of using similar technology has a positive effect on adopting new technology. Yoon (2010)found that customers with a high level of experience get more knowledge ofonline banking systems. A longer length of the relationship is associated with faster adoption of the online channel Estrella-Ramon, Sánchez-Pérez, and Swinnen (2016), when customers use online banking for more services with high frequency, they will realize the importance of adopting security measures.

2.2 Perceived Usefulness (PU) of Security measures to be adopted for safe online banking

The term Perceived usefulness (PU) explains the degree to which a user of technology believes that using the technology would improve the performance of the taskAlKailani (2016). The TAM Model considers the perceived usefulness, and use of use as the main determinants of users' intention towards adopting new technologyAlbert. The customer's perception of the importance and necessity of adopting security measures for safe and secured onlinebanking is the key tothe successful implementation of security in onlinebanking. Customers 'acceptance is essential for the successful implementation of internet banking Alalwan et al. (2018). The findings ofAlbort-Morant, Sanchís-Pedregosa, and Paredes Paredes (2022) statistically proved the explanatory power of customers' perceived usefulness on the adoption of online banking.

2.3 Perceived ease of using (PEU) the security measures of online banking

The term perceived ease of use indicates the degree to which the customer finds the security measures easy in terms of understanding, learning, and adopting. Singh and Srivastava (2020)suggest that onlinebanking should be simple and user-friendly, the customer's intention to adopt onlinebanking is influenced by the perceived usefulnessAlKailani (2016).By designing the security measures as easily adaptable, the customer's adoption level can be improved. A usable online banking security system is associated with lower levels of difficulty in managing itSikdar and Makkad (2015). How the customers find the adoption of security measures easy and user-friendly influences the actual adoption of the onlinebanking security measures recommended by banks such as selecting a secured password, changing passwordsperiodically, and carefully using the system.Kassim and Ramayah (2015), andCHIN, ZAKARIA, PURHANUDIN, and PIN (2021)observed that a user-friendly operating system can result in customers developing a positive attitude towards intentional behaviour, Yoon (2010)found that the ease of use has a positive impact on customer satisfaction and the positive effect has been supported by many e-commerce studies, whereasAlbort-Morant et al. (2022) found the explanatory power of perceived use of using technology on the customer's intention to adopt onlinebanking.Simple and user-friendly onlinebanking applications will motivate and encourage customers to adopt onlinebanking security measures Singh and Srivastava (2020). The security measures are to be user-friendly and not too difficult for the customers to adopt. Abualsauod and Othman (2020) found that the gap between customers' level of technical skills and the requirements for onlinebanking will affect to use of onlinebanking services, therefore the security measures should be implementable at the user level.

2.4 Perceived Risk (PR) of online banking without following security measures

The banking sector constantly upgrading the security mechanism for onlinebanking;however, Cybercrime in Banking sector is a global phenomenon that is also constantly identified and creates security gaps to exploit. Through Phishing and Malware, Cybercriminals aim to deceive the customer or the system tosteal user credentials and/or gain control over customers' onlinebanking devices Jansen and Leukfeldt (2016)**,** Alghazo et al. (2017**).**A large number of customers remain uncertain about internet banking due to its security Obaid (2021), perceived risk is the main barrier to the adoption of internet bankingAlalwan et al. (2018)**,** perceived risk influence the customer's decision over onlinebankingSingh and Srivastava (2020).Musaev and Yousoof (2015)**,**therefore improving security aspects of internet banking becomes vital, the intention to adopt onlinebanking is influenced by the perceived riskAlKailani (2016), the customers should ensure that they use safe and secured onlinebanking platforms Albort-Morant et al. (2022)**,** because the banks cannot have full control of the onlinebanking platforms.

Perceived risk in online banking indicates the degree to which the customer feels the uncertainty and adverse effects of availing the onlinebanking services,Kassim and Ramayah (2015) pointed out that the unique features of internet technology such as distant, impersonal nature and global open infrastructure are capable of creating a lot of uncertainties and risk, Yildirim and Varol (2019)argued that there will be security gaps in every innovation brought by the technology. Polasik and Wisniewski (2009) pointed out that customers may be influenced by the stories of onlinebankingfraud. Realizing the threats of onlinebanking security issues will prompt users to adhere to the security guidelines.

2.5 Attitude (ATT)toward online banking security measures

The Attitude of customers towards onlinebanking measures ultimately influences their adoption of the security measures, Kassim and Ramayah (2015), a more favourable attitude towards online banking leads to using online banking.Attitudes are defined as the user's assessment of the benefice of using the system Safari et al. (2020)**.**The customer's experience in online banking in terms of periods of usage, types, and frequency of transactions, perceived usefulness, perceived use of security measures, and the risk of not adopting security measures will influence the customer's attitude towards onlinebanking security measures. Various studies conducted on customers' adoption of onlinebanking have included attitude as a construct and studied the determinants of attitude and the impact of the attitude on customers' adoption ofonlinebankingSafari et al. (2020)**, CHIN et al. (2021),**AlKailani (2016)&Albort-Morant et al. (2022).

2.6 Intention to adopt security measures (INT)

Intention is a measure of the strength of one's willingness to adopt a particular behaviourKassim and Ramayah (2015), previous studies found a positive impact of intention on the intention to adopt onlinebanking security measuresAlKailani (2016)**,** Al-Ajam and Nor (2015); Albort-Morant et al. (2022)**,** customers' intention to adopt online banking is influenced by their attitude towards online banking, Safari et al. (2020) the attitude influences the intendedbehaviour of existing as well as potential users of online banking, Safari et al. (2020) found that the perceived web security is the main determinant of the intention to use internet banking. Kabir and Islam (2021)**,** security is the essential factor that can inspire customers in using internet banking.

Hypotheses

H 1: Customers' frequency of online banking (FRE) positively influences their attitude towards the security measures suggested bank banks for safe and secured online banking (ATT)

H 2: Customers' frequency of online banking (FRE) positively influences the intention to adopt and continue online banking security measures (INT)

H 3: Perceived usefulness (PU) has a positive effect on customers' attitudes toward adopting online banking security measures (ATT)

H 4: Perceived ease of use (PEU) has a positive effect on customers' attitudes towards adopting online banking security measures (ATT)

H 5: Perceived risk level of online banking without security measures (PR) positively influences the customer's attitude towards adopting online banking security measures (ATT)

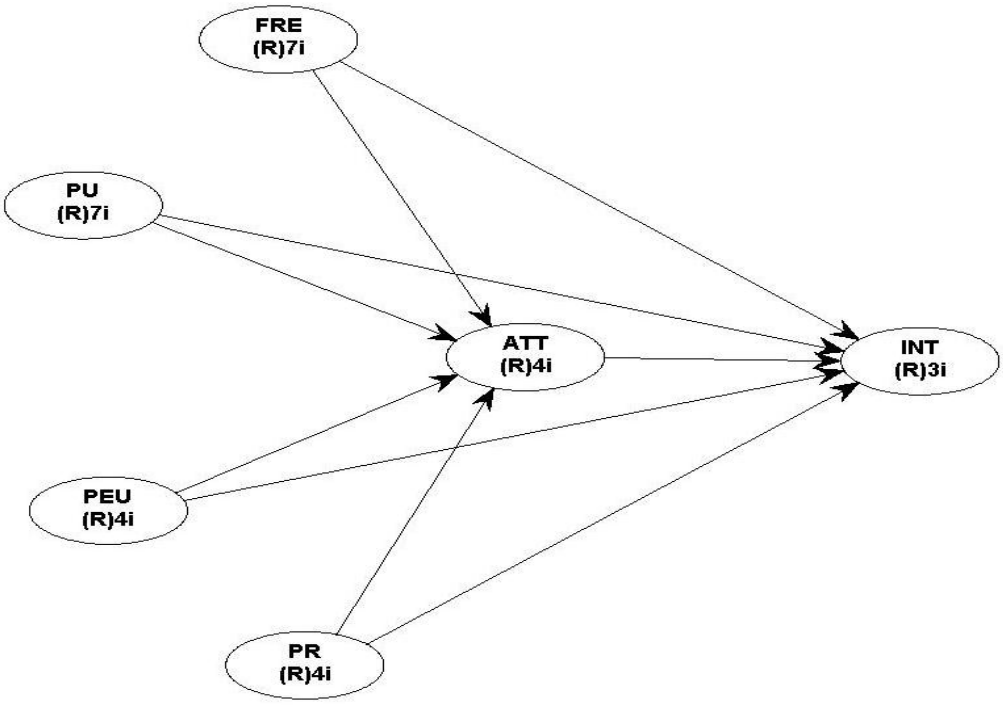
H 6: Perceived risk level of online banking without security measures (PR) positively influences the intentions to adopt and continue online banking security measures (ATT)

H 7: Customers' attitude towards online banking security measures (ATT) positively influences their intention to adopt and continue online banking security measures (INT)

3. Research Model

The research model adopted in this paper is presented in Figure 1. The impact of customers'onlinebankingfrequency, perceived usefulness, perceived ease of using onlinebanking security measures, and the perceived risk of not using the security measures on their intention to adopt and continue onlinebanking security measures are studied by testing seven hypotheses.

Figure 1 Hypothesized Research Model



4. Methodology

4.1 Design and sampling framework and data collection: The Quantitative research design has been adopted in this research with a link to the deductive method by investigating existing literature, theories and developing hypotheses, conducting surveys, and testing the hypotheses through the Extended Technology Acceptance Model (Extended TAM Model) by including frequency and perceived risk of using onlinebanking. The analysis was done using the powerful statistical technique of the Partial Least Square - Structural equation model (PLS-SEM), and the WarpPLS Software 8.00 Version (Latest) was applied to test the model. The data were collected from online banking customers in the Sultanate of Oman through a structured questionnaire. The quantitative method of data collection through a structured questionnaire is the most suitable for studying onlinebanking customers Singh and Srivastava (2020).

By keeping the required power level of 0.800 and selecting the minimum absolute path coefficient with a significance value the WarpPLS Software determined the minimum required sample size of 160 under the Inverse-square root method and 146 underthe Gamma-exponential method.As per the Gama exponential method, the required sample size can be estimated for empirical studies Kock (2021).The questionnaires were distributed to customers of onlinebanking through email, Google survey, and distribution of hard copies, covering all the regions of the country, and collected the responses from 178 customers using onlinebanking. The present study adopted a convenience sampling design, previous research works such asSingh and Srivastava (2020), Safari et al. (2020), CHIN et al. (2021), andKabir and Islam (2021),also adopted convenience sampling.

4.2 Variable Measurement

The questionnaire which was used for the survey consists of three parts (Demographic details of the respondents, Online banking experience in terms of frequency for various services, and Factors affecting the attitude and intention to adopt and continue the online banking security measures. The constructs using reflective measures adopted in this research were developed after reviewing extensive literatureand after making necessary modifications, the constructs were measured on a Likert five-point scale(strongly disagree 1….5 strongly agree). The constructs and items are presented in Tables 1 and 2)

Table 1- Constructs and their sources

Constructs	Number of items	**Source**
Frequency of using online banking **(FREQ)**	7	Giovanis et al. (2012)**,** Polasik and Wisniewski (2009),Yoon (2010)**,** Estrella-Ramon et al. (2016)
Perceived Usefulness of online banking security measures **(PU)**	**7**	AlKailani (2016)**,**Albort-Morant et al. (2022), Alalwan et al. (2018)
Perceived ease of using online banking security measures **(PEU)**	4	Singh and Srivastava (2020),Sikdar and Makkad (2015),Kassim and Ramayah (2015), CHIN et al. (2021)CHIN et al. (2021), Yoon (2010),Albort-Morant et al. (2022), Singh and Srivastava (2020), Abualsauod and Othman (2020)
Perceived risk of online banking without following security measures **(PR)**	4	Jansen and Leukfeldt (2016), Alghazo et al. (2017),Obaid (2021), Kassim and Ramayah (2015),Yildirim and Varol (2019)Polasik and Wisniewski (2009), AlKailani (2016),Albort-Morant et al. (2022), Alalwan et al. (2018)**,** Singh and Srivastava (2020)
Attitude toward adopting online banking security**(ATT)**	4	Safari et al. (2020), CHIN et al. (2021),AlKailani (2016)**,**Albort-Morant et al. (2022),Singh and Srivastava (2020),Kassim and Ramayah (2015),Safari et al. (2020)
Intention to adopt and continue online banking security measures **(INT)**	3	AlKailani (2016),Albort-Morant et al. (2022),Singh and Srivastava (2020),Kassim and Ramayah (2015), Safari et al. (2020)

4.3 Screening data and testing for Common method bias (CMB)

The data are to be screened before applying any statistical analysisHa, Lo, Suaidi, Mohamad, and Razak (2021)**.**In this study, the data were screened through missing value analysisand tested for common method bias**.** The missing value analysis was done through Little missing completely at random (MCAR). If the missing values are more than 15% of the dataset, such responses are to be removed from the analysis, in this study the percentage of missing values is negligible and less than one per cent. The Little's MCAR test done using SPSS showed aChi-square value of 19.658, DF 41, and a Significance value of 0.998, and these values indicate there are no issues of missing value.To check Common method bias (CMB), Harman's single-factor test was conducted. Survey-based research may have a bias when the respondents fill out the survey Singh and Srivastava (2020)**,**The CMB is caused when the respondent's answer to the particular question differs over some time or situation. To check Common method bias (CMB), Harman's single factor test was conducted through exploratory factor analysis on all items of the measured constructs and the extraction sums squared loadingand percentage of variance are at acceptable levels. The percentage of variance should be less than 50%, the test results show 35.97%, therefore CMB was not an issue in the study

5. Results and Discussions

The analysis of the Extended TAM Model done through PLS-SEM using WarpPLS Software Version 8.00 was performed in two stages. Firstly, the Assessment of the measurement model was evaluated by examining the relationship between observed items and latent variables in terms of validity and reliability.

5.1 Assessment of Measurement Model

The reliability, discriminant, and convergent validity of the measurement model are to be statistically tested and this research conducted the assessment by analyzing the values of Structure loading, Composite reliability, Average Variance extraction, and Cronbach alpha. Previous research works for example Musaev and Yousoof (2015), CHIN et al. (2021), Albort-Morant et al. (2022), Singh and Srivastava (2020), Purani, Kumar, and Sahadev (2019),Ha et al. (2021), Chan and Lay (2018),on online banking issues also adopted the same statistical procedure for assessing the measurement model. The loading should be higher than 0.50 Sikdar and Makkad (2015),(Kassim & Ramayah, 2015), the loadings reflect the relevance of the indicatorsAlbort-Morant et al. (2022), andthe loading for all the items in this study is between 0.632 and 0.903 which is well above the acceptable limits.

The Cronbach's alphavalues for all the constructs shown in Table 2 are more than the recommended value of 0.70 Alalwan et al. (2018), Hussain Chandio, Irani, Zeki, Shah, and Shah (2017),**Salem et al. (2019).** The Cronbach's alpha value for PU is 0.757 which is well above the recommended level, but for other constructs (FRE, PEU, PR, ATT&INT) the value is above 0.845. The Composite reliability (CR) shown in Table 2 for the latent variables ranges between 0.847 to 0.926, the values above the acceptable level of 0.70 reflectthat the constructs have an adequate CRAlalwan et al. (2018), **Salem et al. (2019),** which indicates the degree to which the items reflect the latent variablesCHIN et al. (2021), Kassim and Ramayah (2015).

The convergent validity criteria are tested through the Average value extraction (AVE), the AVE for FRE is 0.523, PU 0.576, and PEU 0.582 whereas the value is more than 0.80 for PR, ATT, and INT (Table 2),Albort-Morant et al. (2022)it should be noted that as the AVE values for the five latent variables are more than the acceptable level of 0.50. The CR value should be more than the AVE value(REF19), all the constructs' CR value is more than the AVE value.

The Multi collinearity test is essential in SEM Analysis,Alalwan et al. (2018), andElbaz and Haddoud (2017)itcan be done by analyzing Variance inflation factors (VIF). Previous research works by Alalwan et al. (2018) considered different acceptable levels of VIF, but Kock (2021)recommended that it is acceptable if <= 5, ideally <= 3.3. Table 2 shows the VIF values between 1.612 and 2.953 for FRE, PU, PEU, and PR, these values are within an ideal level, whereas the VIF of ATT and INT are 3.720 and 3.327 respectively, these values are above the ideal level but within the acceptable level of 5.00.

. **Table – 2: Structure Loading, Composite Reliability, AVE, and Cronbach alpha**

Constructs	**Items**	**Loading**	**Composite Reliability (CR)**	**Average Variance Extracted (AVE)**	**Cronbach's Alpha**	**Full collinearity VIFs**
FRE	**FRE1**: Travels and hotel bookings	0.731	0.884	0.523	0.846	1.612
	FRE2: Bill and fees payments	0.661				
	FRE3: Online shopping	0.658				
	FRE4: Online investment transactions	0.632				
	FRE5: Balance inquiry and other inquiries	0.790				
	FRE6: Fund transfer	0.784				
	FRE7: Request for cheque books& others	0.785				
PU	**PU1:** Pick a high-security password and manage it efficiently	0.671	0.904	0.576	0.876	2.196
	PU2: Avoid applications monitoring your details and transactions and open the link via a bookmark.	0.801				
	PU3: After the transaction, logoff, clear the browser's cache, and be vigilant when you use an Internet cafe or other systems	0.799				

	PU4: Use the latest original anti-virus software firewalls systems	0.717				
	PU5: Keep your Identities private and offline and destroy the expired PIN and Bank cards.	0.782				
	PU6: Follow the bank's instructions, regularly check bank statements, and never share account details	0.728				
	PU7: Use payment gates for online shopping	0.803				
PEU	**PEU1:** I can use a secured password, and change it periodically without disclosing it to others	0.828	0.847	0.582	0.757	1.815
	PEU2: I can carefully use the system &adapt the required security measures for online banking	0.807				
	PEU3: It is easy for me to become skillful in adopting security measures of Online banking	0.746				
	PEU4: Overall, I find it easy to follow the security measures of Online banking	0.658				
PR	**PR1:** Account details will be stolen	0.819	0.896	0.684	0.845	2.953
	PR2: It will result in fraudulent financial transactions from my Bank account	0.835				
	PR3: It will lead to uncertainty and vulnerability	0.772				
	PR4: It will result in an unimaginable danger	0.878				
ATT	**ATT1:**Following security measures recommended by banks is a must.	0.903	0.926	0.759	0.894	3.720
	ATT2: I would feel that following security measures for online banking is pleasant	0.873				
	ATT3: In my opinion, following the security measures for online banking is important	0.834				
	ATT4: For a safe and secure online banking experience, adopting security measures is a wise idea	0.872				
INT	**INT1:** I will update myself on the latest security measures for online banking	0.901	0.926	0.806	0.880	3.327
	INT2: I will continue to adopt security measures for my online banking transactions	0.897				
	INT3: I will continue to use and strengthen the security measures of Online banking	0.894				

The relevant and sound measurement instrument is essential for any research, Kock (2021) the quality of the measurement instrument can be authenticated through discriminant validity.The discriminant validity is to be verified by examining the square root of AVEs**,** Al-Ajam and Nor (2015)**,** Hussain Chandio et al. (2017)**,** Kassim and Ramayah (2015)the square root of AVEs should be more than the inter-construct's correlation values.As presented in **Table 3,** the square roots of AVEs – diagonal elements of the correlation matrix are higher than the off-diagonal elements, therefore there is an adequate level of convergent and discriminant validity of the measurement model. Thus, the measurement model demonstrates adequate convergent validity and discriminantvalidity

Table 3: Discriminant Validity - Square roots of average variances extracted (AVEs)

Constructs	FRE	PU	PEU	PR	ATT	INT
FRE	**0.723**					
PU	0.503	**0.759**				
PEU	0.384	0.527	**0.763**			
PR	0.532	0.656	0.605	**0.827**		
ATT	0.558	0.683	0.633	0.768	**0.871**	
INT	0.579	0.677	0.595	0.734	0.791	**0.898**

Note: The squared roots of AVE are shown as diagonal values whereas the off-diagonal values are the estimates of inter-correlation between the latent constructs.

Table 4: HTMT ratios (Heterotrait-monotrait ratio of correlations)

Constructs	FRE	PU	PEU	PR	ATT	INT
FRE	-					
PU	0.580					
PEU	0.480	0.644				
PR	0.627	0.759	0.755			
ATT	0.637	0.771	0.771	0.883		
INT	0.670	0.771	0.725	0.852	0.892	-

The HTMT ratios are applied as a further test for discriminant validity Foroughi, Iranmanesh, and Hyun (2019),HTMT ratios have been proposed by researchers for discriminant validity assessmentKock (2021)**.** If the HTMT ratios of all the constructs fall under the maximum threshold value of 0.85, then the constructs in the proposed path model are conceptually more distinct Chan and Lay (2018). The HTMT values close to 1 indicate a lack of discriminant validity, whereas, **Table 4** shows less than 0.90 for all the constructs, indicating there is discriminant validity of the scales and the questionnaire adopted in this study.

5.2 Assessment of Structural Model

After confirming the reliability and validity of the measurement model Singh and Srivastava (2020)**,** the second stage of PLS-SEM analysis is to assess the structure of the model CHIN et al. (2021)**,** the assessmentis to be done to ensure that the constructs used in the model is pertinent and measure the relationships. Path coefficient results are reported in Table 7 based on the results from the PLS structural model after reliability and validity of the measurement were assured

Figure 2 Structural Model

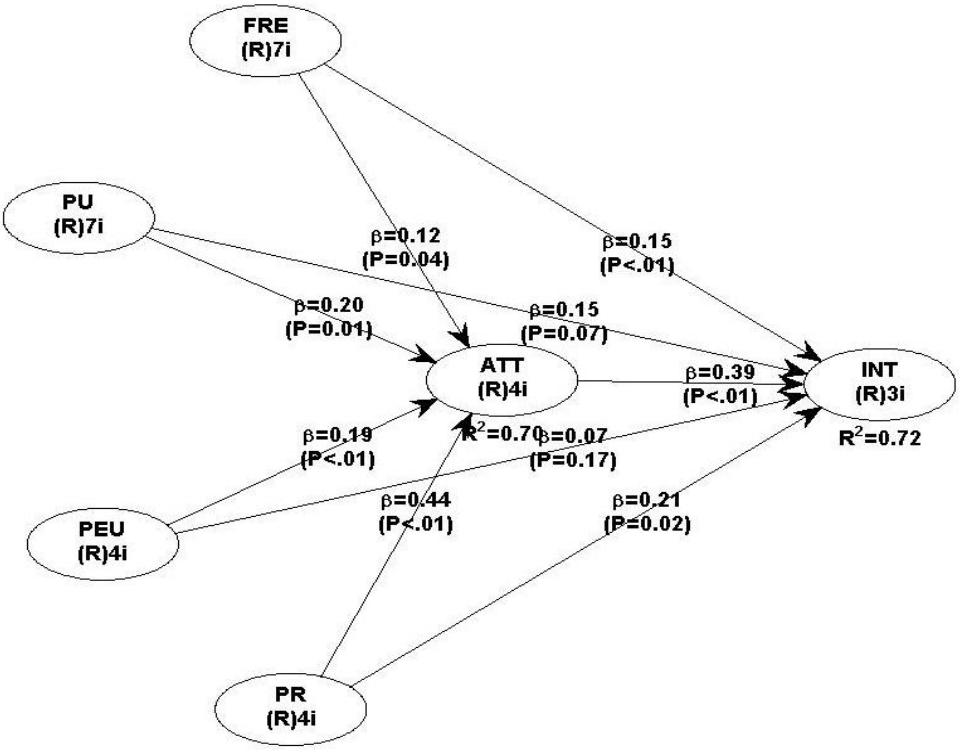


Table 4 Path coefficients

Hypotheses	Path	Path coefficient	p values	T ratios for path coefficients(Critical T ratio = 1.645)	Remarks
H 1	FRE → ATT	0.125	0.04	1.721	H1 Supported
H 2	FRE → INT	0.149	<0.01	2.872	H2 Supported
H 3	PU → ATT	0.201	0.01	2.227	H3 Supported
H 4	PEU → ATT	0.193	<0.01	2.730	H4 Supported
H 5	PR → ATT	0.443	<0.01	4.976	H5 Supported
H 6	PR → INT	0.211	0.02	2.067	H6 Supported
H 7	ATT → INT	0.386	<0.01	4.906	H7 Supported

To test the theoretical model of the research, PLS-SEM with Bootstrapping method was applied using WarpPLS Software (Version 8.0). The path coefficients, p values, and T ratios are presented in Table 4, whereas Table 5 shows the mediation effect (bothdirect and indirect effect). The significance of path coefficients can be analyzed in terms of p values and **t** values. When the empirical **t** values are higher than the critical values, we can state that the coefficient is statistically significant. The one-tailedtest critical T ratios value is 1.645, whereas the T ratio values of path coefficients shown in Table 4are higher than the critical T ratios.

The frequency (FRE) of using online banking by customers is influencing their attitude (ATT) towards online security measures, the path FRE → ATT with a coefficient value of 0.125 is significant with a p-value of 0.04 and the T ratio is 1.721 supporting the significance as the T ratio is more than the critical level of 1.645(Table 4). The impact of FRE on INT (customers' intention to adopt and continue security measures) is more than the impact on ATT asrevealed by path coefficient 0.149, p-value<0.01, and T ratio 2.872 (Table 4). The perceived risk (PR) of not adopting online banking security measures has an impact on INT, the path PR → INT with coefficient value 0.211 and p value 0.02 is significant and the T ratio of 2.067 support the p-value, similar results were found by Singh and Srivastava (2020)

Similarly, the path PR → ATT is also significant with a p-value<0.01, coefficient of 0.443, and T ratio of 4.976, these results are in line with the results ofKassim and Ramayah (2015),Nguyen and Nguyen (2017),Safari et al. (2020)**.** Both FRE and PR have an impact on INT, the customers who use online banking frequently for various transactions have a positive attitude toward the security measures of online banking and realize the evil effects of using online banking without security measures. The impact of perceived usefulness (PU) and perceived ease of use (PEU) of online banking security measures on ATT is statistically proved as revealed by the path coefficient values, p-value, and T ratios of path PU → ATT and PEU → ATT. (Table 4). Figure 2 shows that the direct impact of PU and PEU on ATT is not statistically significant, this is in with the findings of Albort-Morant et al. (2022)**,**Sikdar and Makkad (2015)**,** and Kassim and Ramayah (2015),the resultsofCHIN et al. (2021)statisticallysupport the effect of path PU →ATT but not the path PEU → ATT.The path → INT with coefficient value of 0.386, p-value<0.01, and T ratio of 4.906 is statistically proven, these results are supported by the results of Tarhini et al. (2016)**,** Alalwan et al. (2018)**,** Salem et al. (2019)**,**Foroughi et al. (2019),Safari et al. (2020)**,**Sikdar and Makkad (2015).

5.3 Mediation Analysis

The mediation analysis underwent many advancements Rijnhart et al. (2021)**,**and it explains the indirect effect of the independent variable on the dependent variable via another independent variable. The mediation effect was examined in this study by analyzing the path coefficient values and their significance value at 5%. The mediation is strong and called full mediation when there is an indirect effect but no direct effect, when there is both direct and indirect effect, it is said to be partial mediation Zhao, Lynch Jr, and Chen (2010)**,** CHIN et al. (2021)**.** Table5 shows the statistics of the direct effect and indirect effects of path FRE → INT, PU → INT, PEU → INT, and PR → INT. The path FRE → INT has both direct effects as well as statistically significant indirect

effects, therefore it is concluded that the mediation is partial. The direct effect has a 0.149 path coefficient at a p-value<0.01, whereas the indirect effect's path coefficient value is 0.048 with a p-value of 0.042, the direct effect is more powerful than the indirect effect, because when the customer's usage level of online banking increases, it brings interest and seriousness of adopting and continuing security measures. Similarly, the path PR → INT has a higher path coefficient for its direct effect than the indirect effect, because when the customer's perceived risk level of online banking is high, they have a strong intention to adopt and continue security measures. The direct effect of path PU → INT and PEU → INT is not statistically significant, whereas the indirect of this path has statistically significant with p values 0.011 and 0.012 resultantly these paths have full mediation, however,Albort-Morant et al. (2022) statistically proved significant direct and indirect effect of path PEU → INT.

Table 5 Mediation effect (Indirectand direct effects)

Path	**Direct effect**		**Indirect effect via Attitude**		**Outcome**
	Path coefficient	P values	Path coefficient	P values	
FRE → INT	0.149	<0.01	0.048	0.042	Partial mediation
PU → INT	0.152	0.07	0.077	0.011	Full mediation
PEU → INT	0.072	0.17	0.074	0.012	Full mediation
PR → INT	0.211	0.02	0.171	<0.001	Partial mediation

Table 6 Confidence intervals for path coefficients

Path	Confidence intervals for path coefficients	
	Lower level	Upper level
FRE → INT	0.047	0.251
PU → ATT	0.024	0.377
PEU → ATT	0.054	0.331
PR → INT	0.011	0.412
ATT → INT	0.232	0.540

Table 6 shows the confidence intervals for path coefficients of direct effects between the latent variables given in the table at a 95% confidence level, as the values are in the same sign it indicates the certainty of the estimate, Ahmed, Streimikiene, Channar, Soomro, and Streimikis (2021) and there is no value of zero between the lower and upper interval.

6. Implications of the study

This study brings out the required conceptual and empirical clarity about online banking customers' behaviourregarding the security measures suggested by commercial banks. to the factors. This study has several important theoretical and practical implications for online banking activities.The present study has many implications for future studies on the security of online banking. The empirical results show that the customer's frequency of using online banking and their risk perception of not using online banking influences their attitude as well as intention towards adopting online banking security measures. But the perceived use and perceived ease of use can directly influence their attitude towards security measures but not the intention to adopt them. The TAM Extended model using Structural Equation Model has significant explanatory power and is capable of generating good results to understand the antecedents.

The TAM (Technology Acceptance Model) has been extended with two important constructs (Frequency of using online banking and the perceived risk of using online banking without adopting security measures), these two constructs were not applied in the previous studies. Expanding customer and service networks, minimizing cost, and delivering value to customers through online banking can be achieved only through offering safe and secured

online banking, Albort-Morant et al. (2022) it is essential to act on cyber-risks that could jeopardize online banking. Strengthening the security measures, and reinforcing customers' adoption of security measures makes online banking reliableKhan et al. (2017)**.**The benefits of sophisticated and highly secured online banking platforms become meaningful and relevant only when the customers make use of it. This study's findings will certainly help commercial banks to understand the customer's attitude and usage level of online banking security measures, accordingly, they can initiate further actions toward successful implementation of the security measures.

7. Limitations of the study and scope for further study

Notwithstanding the main findings and contributions of our study, this paper has limitations relating to the scope of the sampling design, as the study focused on the adoption of online banking security measures, it focused only on existing online banking customers, however further studies can extend the scope to cover the prospective online banking customers also. As there is a paucity of empirical research on online banking measures, the present study could not extend the scope of analysis covering the moderating variables, therefore future studies can be extended by including the moderating role of gender, education, etc. To develop the construct of PU (perceived use of online banking security measures) the study adopted seven latest and important security measures suggested by commercial banks in Oman has been selected as items of the construct. For future studies the type and number of items to develop the PU constructs can be updated as per the recommendations of the banks,Montazemi and Qahri-Saremi (2015)the measures identified for each factor can vary for empirical studies.

8. Conclusion

The system of online banking is ever-changing and it is interesting and essential to investigate how the customers perceive and react to the changes. Among the various factors affecting online banking adoption, the customers perception over usefulness easy of using and the risk mainly influence the adoption process of online banking and relevant security measures. This study investigated customers frequency of online banking, perceived use, ease of using security measures and the risk of not adopting security on their attitude towards security measures and their intention to adopt security measures.

The results show that customers who use online banking frequently for transactions such as travel and hotel bookings, bill and fee payments, online shopping, online stock market, investment transactions, and fund transfer have a positive attitude about security measures of online banking and intend to adopt and continue security measures. Therefore, bankers should encourage and educate further about updated security measures for safe and secure online banking. Customers with high awareness levels about the dangers of not adopting security measures have a positive attitude about the importance of security measures and they intend to continue the security measures. The latent variable of perceived usage of online banking security measures was measured with seven items of essential security measures suggested by the leading commercial banks in Oman with higher presence in online banking, The perceived usage (PU) and perceived ease of using (PEU) online banking security measures have significantly influenced the attitude (ATT) of customers towards the security measures and in turn, the ATT significantly influence the customers' intention (INT) towards adopting and continuing online banking security measures. However, these two constructs could not influence the ATT directly, therefore the commercial banks have to take initiative to make the customers understand the dangers of not adopting online banking security measures and adequately educate them on the latest and proper security measures. Educating customers about the need and importance of adopting suggested security measures for safe and secured online banking is vital.

References

1. *Abualsauod, E. H., & Othman, A. M. (2020). A study of the effects of online banking quality gaps on customers' perception in Saudi Arabia. Journal of King Saud University-Engineering Sciences, 32(8), 536-542.*
2. *Ahmed, R. R., Streimikiene, D., Channar, Z. A., Soomro, R. H., & Streimikis, J. (2021). E-Banking Customer Satisfaction and Loyalty: Evidence from Serial Mediation through Modified ES-QUAL Model and Second-Order PLS-SEM. Engineering Economics, 32(5), 407-421.*
3. *Al-Ajam, A. S., & Nor, K. M. (2015). Challenges of adoption of internet banking service in Yemen. International journal of bank marketing.*

4. *Al-Fahim, N. H. (2012). Factors affecting the adoption of internet banking amongst IIUM'students: a structural equation modelling approach. Journal of Internet Banking and Commerce, 17(3), 1.*
5. *Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Algharabat, R. (2018). Examining factors influencing Jordanian customers' intentions and adoption of internet banking: Extending UTAUT2 with risk. Journal of Retailing and Consumer Services, 40, 125-138.*
6. *Albort-Morant, G., Sanchís-Pedregosa, C., & Paredes Paredes, J. R. (2022). Online banking adoption in Spanish cities and towns. Finding differences through TAM application. Economic Research-Ekonomska Istraživanja, 35(1), 854-872.*
7. *Alghazo, J. M., Kazmi, Z., & Latif, G. (2017). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. Paper presented at the 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS).*
8. *AlKailani, M. (2016). Factors Affecting the Adoption of Internet Banking in Jordan: An Extended TAM Model. Journal of Marketing Development & Competitiveness, 10(1).*
9. *Aribake, F. O. (2015). Impact of ICT tools for combating cybercrime in Nigeria online banking: a conceptual review. International Journal of Trade, Economics and Finance, 6(5), 272.*
10. *Chan, S. H., & Lay, Y. F. (2018). Examining the reliability and validity of research instruments using partial least squares structural equation modelling (PLS-SEM). Journal of Baltic Science Education, 17(2), 239.*
11. *Chandio, F. H., 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.*
12. *Chen, H., & Corriveau, J.-P. (2009). Security testing and compliance for online banking in the real world. Paper presented at the Proceedings of the International MultiConference of Engineers and Computer Scientists.*
13. *CHIN, K. Y., ZAKARIA, Z., PURHANUDIN, N., & PIN, C. T. (2021). A Paradigm of TAM Model in SME P2P Financing. International Journal of Economics & Management, 15(3).*
14. *Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.*
15. *de Oliveira Santini, F., Ladeira, W. J., Sampaio, C. H., & Perin, M. G. (2018). Online banking services: A meta-analytic review and assessment of the impact of antecedents and consequents on satisfaction. Journal of Financial Services Marketing, 23(3), 168-178.*
16. *Elbaz, A. M., & Haddoud, M. Y. (2017). The role of wisdom leadership in increasing job performance: Evidence from the Egyptian tourism sector. Tourism management, 63, 66-76.*
17. *Estrella-Ramon, A., Sánchez-Pérez, M., & Swinnen, G. (2016). How customers' offline experience affects the adoption of online banking. Internet Research.*
18. *Foroughi, B., Iranmanesh, M., & Hyun, S. S. (2019). Understanding the determinants of mobile banking continuance usage intention. Journal of Enterprise Information Management.*
19. *Giovanis, A. N., Binioris, S., & Polychronopoulos, G. (2012). An extension of the TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. EuroMed Journal of Business, 7(1), 24-53.*
20. *Ha, S. T., Lo, M. C., Suaidi, M. K., Mohamad, A. A., & Razak, Z. B. (2021). Knowledge Management process, entrepreneurial orientation, and performance in SMEs: Evidence from an emerging economy. Sustainability, 13(17), 9791.*
21. *Hu, W., & Khanam, L. (2016). The Influence of Cultural Dimensions and Website Quality on m-banking Services Adoption in Bangladesh: Applying the UTAUT2 Model Using PLS. Paper presented at the Association for Information Systems.*
22. *Hussain Chandio, F., Irani, Z., Zeki, A., Shah, A., & Shah, S. (2017). Online Banking Information Systems Acceptance: An Empirical Examination of System Characteristics and Web Security.*
23. *Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79.*

24. *Jiang, M., Rifon, N. J., Cotten, S. R., Alhabash, S., Tsai, H.-Y. S., Shillair, R., & LaRose, R. (2022). Bringing older consumers onboard to online banking: a generational cohort comparison. Educational Gerontology, 48(3), 114-131.*
25. *Kabir, M., & Islam, M. (2021). Extension of TAM explaining the determinants of I-banking adoption: Bangladesh perspective. Paper presented at the AIP Conference Proceedings.*
26. *Kassim, N. M., & Ramayah, T. (2015). Perceived risk factors influence the intention to continue using internet banking among Malaysians. Global Business Review, 16(3), 393-414.*
27. *Khan, I. U., Hameed, Z., & Khan, S. U. (2017). Understanding online banking adoption in a developing country: UTAUT2 with cultural moderators. Journal of Global Information Management (JGIM), 25(1), 43-65.*
28. *Kock, N. (2021). WarpPLS user manual: version 6.0. Laredo, TX: ScriptWarp Systems.*
29. *Makanyeza, C., & Mutambayashata, S. (2018). Consumers' acceptance and use of plastic money in Harare, Zimbabwe: Application of the unified theory of acceptance and use of technology 2. International journal of bank marketing, 36(2), 379-392.*
30. *Montazemi, A. R., & Qahri-Saremi, H. (2015). Factors affecting adoption of online banking: A meta-analytic structural equation modelling study. Information & management, 52(2), 210-226.*
31. *Musaev, E., & Yousoof, M. (2015). A review on internet banking security and privacy issues in Oman. Paper presented at the Proceedings of the 7th International Conference on Information Technology (ICIT 2015), Chiang Mai, Thailand.*
32. *Nguyen, T. D., & Nguyen, T. C. (2017). The role of perceived risk on intention to use online banking in Vietnam. Paper presented at the 2017 international conference on advances in computing, communications and informatics (ICACCI).*
33. *Obaid, T. (2021). Predicting Mobile Banking Adoption: An Integration of TAM and TPB with Trust and Perceived Risk. Available at SSRN 3761669.*
34. *Olalere, M., Waziri, V. O., Ismaila, I., & Ololade, O. (2014). Assessment of Information Security Awareness among Online Banking Costumers in Nigeria. International Journal of Advanced Research in Computer Science and Software Engineering.*
35. *Pakojwar, S., & Uke, N. (2014). Security in online banking services—A comparative study. International Journal of Innovative Research in Science, Engineering and Technology, 3(10), 16850-16857.*
36. *Polasik, M., & Wisniewski, T. P. (2009). Empirical analysis of internet banking adoption in Poland. International journal of bank marketing.*
37. *Purani, K., Kumar, D. S., & Sahadev, S. (2019). e-Loyalty among millennials: Personal characteristics and social influences. Journal of Retailing and Consumer Services, 48, 215-223.*
38. *Rijnhart, J. J., Lamp, S. J., Valente, M. J., MacKinnon, D. P., Twisk, J. W., & Heymans, M. W. (2021). Mediation analysis methods used in observational research: a scoping review and recommendations. BMC medical research methodology, 21(1), 1-17.*
39. *Safari, K., Bisimwa, A., & Armel, M. B. (2020). Attitudes and intentions toward internet banking in an underdeveloped financial sector. PSU Research Review.*
40. *Salem, M. Z., Baidoun, S., & Walsh, G. (2019). Factors affecting Palestinian customers' use of online banking services. International journal of bank marketing.*
41. *Sikdar, P., & Makkad, M. (2015). Online banking adoption: A factor validation and satisfaction causation study in the context of Indian banking customers. International journal of bank marketing, 33(6), 760-785.*
42. *Singh, S., & Srivastava, R. (2020). Understanding the intention to use mobile banking by existing online banking customers: an empirical study. Journal of Financial Services Marketing, 25(3), 86-96.*
43. *Tang, C. Y., Lai, C. C., Law, C. W., Liew, M. C., & Phua, V. V. (2014). Examining key determinants of mobile wallet adoption intention in Malaysia: an empirical study using the unified theory of acceptance and use of technology 2 models. International Journal of Modelling in Operations Management, 4(3-4), 248-265.*
44. *Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modelling approach. Information Technology & People.*

45. *Vuković, M., Pivac, S., & Kundid, D. (2019). Technology acceptance model for the internet banking acceptance in the split. Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy, 10(2), 124-140.*
46. *Yildirim, N., & Varol, A. (2019). Research on security vulnerabilities in online and mobile banking systems. Paper presented at the 2019 7th International Symposium on Digital Forensics and Security (ISDFS).*
47. *Yoon, C. (2010). Antecedents of customer satisfaction with online banking in China: The effects of experience. Computers in Human Behavior, 26(6), 1296-1304.*
48. *Zhao, X., Lynch Jr, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. Journal of consumer research, 37(2), 197-206.*