INTERNATIONAL DEVELOPMENT PLANNING REVIEW
ISSN:1474-6743 | E-ISSN:1478-3401

THE DIGITAL BANKING DILEMMA: EVALUATING SECURITY CONCERNS AND CUSTOMER TRUST IN RAJASTHAN'S PRIVATE SECTOR BANKS

Riya Goswami[1], Dr. Pushpkant Shakdwipee[2]
Research Scholar[1], Faculty of Commerce, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan 302017, India
Associate Professor[2], Pacific Institute of Management, Pacific University, Udaipur
Email: riyagoswami422@gmail.com[1]
pushpkant1976@gmail.com[2]

Abstract

The role of technology and digitalisation on the entire world has been quite evident from the previous research conducted. However, the prime focus when it comes to India is that of the cyber security issues that prevails all over. The previous literature paid more attention towards the adoption of digital banking among individuals with respect to the effectiveness and efficiency of the process. Using 405 digital banking customers from private banks in Rajasthan, the study extracts the critical factors and identifies the relationships it holds with customer trust. In case of security and privacy, it is seen that the regression model generated is statistically significant with a p-value of less than 0.05. The adjusted R^2 at 0.537 represents 53.7% variance caused by the independent factors on the levels of security and privacy about digital banking services in private banks. In case of the perception about trust a similar pattern is observed among the customers. The adjusted R^2 in this case stands at 0.470 which is the level of variance explained by the independent factors. Further investigation shows that the first four challenges namely Un-updated information on the internet sources, making fraud and scam calls, Unauthorized access to the bank account and down server of banks impact on the trust levels of the customers about the security that the bank's digital banking methods are able to provide.

Keywords – Digital Banking, Trust, Customer Privacy

1. Introduction

Digital modes of operating in the financial system today have become the minimum requirement for any customer. The financial sector which broadly comprises banks, financial and insurance institutions have opted for a system of regulation that is based entirely upon the technological methods (Windasari et al., 2022). The banking sector is one of the largest industrial categories across the world. It facilitates millions of customers to reach their banking requirements and help to achieve financial stability. Banking sector not only caters to the savings opportunities but also includes schemes for credit taking and browsing through investment opportunities. The banking sector follows strict regulatory guidelines that allows them to serve their customers with ease. However,

in the past decade, the world was disrupted with the era of online services. From shopping online to banking online, everyone today has accepted the fact that they can browse their needs and requirements through the internet (Dutta & Sarma, 2021). The banking industry too was revolutionised with this change and it began the mark of an era of digital banking.

The world of cyber security has increased its approach in the present times due to the increase in the number of digital banking uses (Jain et al., 2021). The history of cybersecurity goes back to 1999 when the computers were developed and viruses attacking the systems have been recognised by the developers. Since then, the issue of cybersecurity has been taken into consideration quite seriously with proper legal formulations developed to tackle them. Cybersecurity can be addressed in terms of three critical components – integrity, confidentiality and availability (Ghate & Agrawal, 2017). The breach of the cybersecurity levels can impact on the stakeholders of Information and Communication Technology (ICT) at different levels. It can cause personal identity theft, lead into fraud, businesses phase the risk of being subjected to intellectual property breaches etc.

In India the cyber law system has been designed to reduce the number of mishaps. The Information technology Act 2000 deals with the issues of cybersecurity and includes 94 sections covering the required crimes. For instance, section 66 states that there would be an imprisonment up to three years with fine up to five lakh rupees on being guilty of hacking a computer system (Ghate & Agrawal, 2017). While all these sections have been drafted to protect the rights of the consumers, the awareness about the same among the majority of the people are found to be lacking.

In terms of banking, the following security issues can arise for the customers –

1. Cybersecurity Threats: As discussed above, the most common form of security issues arising in the use of digital banking are the threats one receives from browsing the sites of the respective banks. They might imbibe phishing attacks, hacking from unknown strong cyber hackers, be victim to malware practices etc. The risk of these breaches is quite high as these data breaches can directly lead to losing the financial inheritance of the customers. This acts as one of the prime reasons of undergoing financial fraud due to unauthorised access of information.

2. Identity Theft: The next high-risk crime rising out of security breaching in the digital banking system includes the identity theft of the customers. In this particular case, the customers might be stripped of their identity and transmit their personal and financial information to themselves. Once this information is accessed, it becomes easy to conduct fraudulent activities in the usage of digital banking methods.

3. Data Breaches: The next set of breaches is about the mismanagement of customer information when using digital banking. When a customer is a prey to data breach, the hackers can expose sensitive data of the customer such as their bank passwords and PINs to others. The account details might be exposed to others which pave way for many security breaches.

4. Mobile Device Security: The digital banking system extends into providing customers with very appropriate mobile banking options. This leads to the increased need for mobile device security. The issue of stolen phones is quite common in India and with the mobile banking applications being browsed through them, the risk of losing important financial information always remains with the customers.

5. Transaction Security: The use of digital banking methods includes making third party payments through the banking platform itself. The fund transfers to other parties takes the customers to payment gateways that do not belong to the bank. Although there are authentication procedures and encryptions, these too can sometimes lead to breach of security and customers falling victim to cybersecurity.

6. Regulatory Compliance: The IT Act 2000 provides a guideline on the use of the internet even for digital banking purposes. There might be failure among the digital banking customers to adhere to these regulations which can lead to the customers facing legal consequences and fines for their actions.

7. User Awareness and Education: In the pursuit of adopting a digital economy, the lack of awareness among users often poses potential security threats. The implementation of best practices for secure online behaviour can contribute to security issues. Educating customers about digital usage is of utmost necessity.

The above issues are some of the common instances that can lead to the breach of security in the digital banking usage. While studies have been conducted to understand the barriers to the adoption of digital banking, there are few that provide a detailed understanding about the security issues that can contribute to the intention of using these modes of transactions. The study would focus on addressing the same and the specific geographical arena where the study is to be conducted is the state of Rajasthan.

The research question attempted in the study is –

RQ1: What are the challenges that the customers face when using the digital banking method for Indian banks?

RQ2: How do security and privacy concerns regulate the digital banking adoption for Indian banks?

2. Review of Literature

The literature across the world has been focusing on the digital aspect of banking since it gathered pace in the last ten years. From understanding its methods of working to determining the factors that impact it taking on among people from all over, the research in the area is well constructed. However, the list of challenges in it taking on are ever increasing and needs to be updated from time to time. Today is an era of digital revolution and along with it comes a different nature of challenge towards Digital Banking. The study here would understand the challenges of taking on Digital Banking in reference to security and privacy concerns.

This study is aimed to make a detailed investigation in the field and deduct the appropriate research gaps.

(Haryono et al., 2023) initiated a study to determine the challenges of Digital Banking with reference to the rapidly growing digital phenomenon. The study here is based on qualitative methods where the reviews are conducted by analysing reports, articles, books, interviews and other such news to understand the challenges in detail. Out of the challenges reported it is found that the level of competition among the banks is now extended to other financial entities. It has led to intense competition and the pressure to provide its users with better technology and a sense of security adds to these challenges.

(Rahman et al., 2023) did their study specifically to understand the impact caused by the use of artificial intelligence in the banking service which is a part of the Digital Banking realm. A total of 306 responses from bank customers of Malaysia have been selected to be analysed quantitatively for the purpose of the study. The results of the study shows that fraud detection and mitigation of risk can be essential components that can be overcome by the use of AI in the banking sector. However, the intention to adopt such facilities are significantly regulated by the perceived risk (PR), the perceived usefulness (PU) and the subjective norms associated with every customer.

(Aidonojie et al., 2022) involved in a study that pointed out the challenges in the Nigerian Digital Banking situation along with understanding the legal issues surrounding the same. The use of DB as a result of globalisation has been made quite familiar in the Nigerian banking system as well. The study used a total of 306 primary responses from individuals residing in Nigeria. The study analysed the collected responses and have been able to specify that out of all the list of problems, the lack of proper internet infrastructure is one of the prime reasons for concern.

(Patnaik et al., 2023) in their study focused upon the taking on of digital payments by the Indian customers while investigating the factors that impact on them. The use of digital payments has been made quite frequently in the Indian infrastructure of finance and more users are being detected in the form in the recent years. With a total of 426 primary data said, the investigation has been made by quantitatively deriving the factors that impact on the taking on of digital payments.

(Saxena et al., 2023) did the study to find both the reasons for use as well as the challenges restricting the use of mobile banking in India. The study developed in the quantitative method used to TAMs and combines them to deduct the factors affecting the taking on of Mobile Banking. As a part of the study a total of 536 responses have been collected from the Delhi and NCR region from Mobile Banking customers. The barriers

that are found include the security levels associated with its use, the level of discomfort in taking it as a medium of banking and cognitive resistance leading to behavioural changes towards Mobile Banking.

(Kaur et al., 2021) did the study in northern India with respect to Digital Banking to find out the challenges specific to the customers deciding in those areas. With the pandemic, the use of Digital Banking methods has increased to a substantial level and have led to more and more users opting for these methods. The study used a total of 222 responses from banking customers of northern India to highlight the focus points of their idea of Digital Banking. The study has shown that the customers are highly satisfied with the Digital Banking services they are using and they consider them to be low on risk.

(Li et al., 2021) have learnt about the use of e-banking services by the customers and the levels of satisfaction that they are deriving from it. The emergence of cloud services to facilitate the banking transactions of the customers is the idea behind conducting this particular investigation. Out of the four factors influencing e-banking includes security along with cloud services, the service quality provided and the e-learning methods facilitated. This shows that security concerns lying with respect to the e-banking services is quite essential to consider. This can immensely impact on the levels of satisfaction derived. Further, with a higher level of satisfaction, there can be increased chances of a customer using the e-banking services repeatedly in the future. The study has been conducted using SEM and all these factors extracted are based on statistical insights.

(Ngoc Thach et al., 2021) did a case study in the Vietnamese banking sector by understanding the risk associated with the taking on of online banking methods. The quality management in terms of the use of technology while addressing the cyber security concerns have been highlighted in the course of the study and have worked through different methods in which it can be achieved. The vulnerabilities associated with the use of the Internet for banking transactions is quite high because of age and optimum maintenance of the quality of technology is very essential in this regard.

(Jünger & Mietzner, 2020) generated their study to understand about the taking on of FinTech services by the households in Germany. The study has been designed to know more about the taking on of the new technological methods being adopted by these households in reference to the financial institutions including banks. In the survey conducted it is by around 31% of the total respondents that have agreed to adopting a new mode of financing rather than the traditional methods. Among the factors that are found to have significantly impacted on the service taking on include trust.
Existing studies in the field have highlighted the importance of digital banking and how in the upcoming years with its different approaches would be the main form of making

banking transactions. Whether it is Mobile Banking services or the different digital payment methods initiated by the banks, the use of digital banking would be necessary for every banking customer in the near future.

In response to this unavoidable necessity in the future, the study here would make an attempt to bridge the gap that is found to be existing in the current state of literature. Firstly, there are different digital banking methods that have been continuously introduced to the users but the updated literature is not available in an area where the banking customers are used to the technological advancements. Most of the studies are from the time when it was an early stage for customers, especially in the emerging countries to digital banking methods and it now needs to be upgraded in an area where the customers are equipped and have an understanding capability about the same. The number of studies that directly point out the challenges in adoption of digital banking is quite scarce as compared to the studies focusing on identifying the factors enhancing their use. Both the positive and negative aspects of adopting digital banking are required and it is important that the number of studies identifying the challenges in detail is being provided. Further, the study is interested in specially looking at the population of Rajasthan which is a growing state in the country of India including a high level of rural population. The problem of digital divide has also been highlighted in the study and in order to bridge the gap the study of challenges in adopting digital banking in a state like Rajasthan would be eye-opening.

Overall, the above literature shows that there are very few studies which exclusively points to the challenges of Digital Banking adoption and that too in an emerging economy where the number of Digital Banking users are still increasing at a very high rate.

3. Research Methodology

The research employs a quantitative approach, which proves advantageous in quantifying the determinants of the study. The study utilizes a structured questionnaire developed from existing literature, incorporating questions adapted from scales employed by previous researchers. These questions are tailored to suit the specific needs of the study and are presented in a 5-point Likert scale format.

The sampling population serves as one of the important parts in the entire study. The study here is focusing in the city of Jaipur with the focus on the customers of the following private sector banks-

1. **HDFC Bank (**Revenue: ₹ 148365 Cr)
2. **ICICI Bank (**Revenue: ₹ 104322 Cr)
3. **Axis Bank Ltd (**Revenue: Rs 80,847 Cr)
4. **Kotak Mahindra Bank** (Revenue: Rs.56,814 Cr)

These banks have been selected specifically out of the 21 Indian private banks based on their revenue. The top 4 revenue generating private sector banks have been considered for the study.

Out of the two main categories of sampling, the study would use simple random sampling to collect data from the respondents. This falls under the probabilistic method of study and ensures that the samples collected are unbiased and picked up randomly from the customers who are using the digital banking services of the above-mentioned private banks.

For the purpose of the study a total of 400 responses would be collected after considering the requirements of the Cochran's formula of sample size determination.

4. Results & Discussion

There are a total of 405 customer datasets considered which do not include any missing value and using advanced statistical procedures, the objectives would be fulfilled.

There are four age groups observed where the highest number of digital banking customers belong to 35 to 44 years of age with 25.7% of the total respondents. There are 22.2% in the 45 to 54 years of age group and 21.55 each for 18 to 24 and 25 to 34 years of age. There are 9.1% who belong to above 55 years of age. The educational qualification shows that with 45.2%, the majority of the respondents are graduates followed by 31.1% post graduates. There are 19% in the senior secondary levels and 4.7% hold other degrees.

In case of the frequency of digital transactions which are investigated in terms of month wise engagement shows that 36% use it around 16 to 20 times a month. There are 21.2% who engage in it more than 20 times a month. There are also 21.55 who only use it less than 5 times a month. The frequency shows that there are a diverse set of users for digital banking where the frequency of usage varies significantly.

The research objective is stated as follows –

1. To analyse the impact of cybersecurity incidents on consumer perception regarding the security and trust in digital banking.

Firstly, there are 24 items used to measure various aspects of cybersecurity in the banking sector. This is followed by a 7 item scale that specifies the list of challenging factors that hamper the cybersecurity measures in a digital banking scenario. In order to ascertain the ability of these items in the Likert Type scale to measure each of the considered variables effectively, a reliability analysis is conducted. The consideration taken for understanding the reliability of the overall scale and its individual items, Cronbach's Alpha value is taken.

As per (Hair et al., 2006), the Cronbach's Alpha value of more than 0.7 denotes a high reliability for the scales. Here, the overall reliability stands at 0.789 along with item wise values showing acceptable results. This denotes the achievement of reliability for the considered items in the scale and can be taken for further analyses.

The sampling adequacy tests show that in Bartlett's test a p-value of less than 0.05 and an overall KMO of 0.881 is generated. This fulfils all the conditions of sampling adequacy as stated by (Hair et al., 2006). Hence, the section explains the results of the Principal Component Analysis (PCA) conducted for factor extraction.

There are a total of six factors extracted from the list of 31 items and all the individual items have a factor loading of more than 0.4 which means all are to be included in factor composition.

The table below represents the six extracted factors and their details.

Table 1 – List of Factors

Factor Name	No. of Items	Description
Security & Privacy	**5**	**This factor represents the ability of the private banks to protect the privacy of the customers in their digital banking initiative and provide security**
Trust	**5**	**It represents the level of trust that the customers can show towards the online banking facilities provided by their banks**
Innovativeness	**4**	**This factor refers to the level of innovativeness shown by digital banking services of the private banks over the traditional services earlier being provided**
Awareness	**3**	**It states the level of awareness provided by the private banks to their customers about the safety and security of their online information and transactions**
Data Protection	**7**	**These items include the different measures that are considered essential by the customers for data protection**
Challenging Factors	**7**	**This factor lists out the challenges that the customers are facing when trying to have a secure digital banking experience.**

These six factors are now statistically validated and would be used in the analysis to identify different aspects of cybersecurity in private banks.

Considering each of the six factors and exploring their item wise mean scores, a number

of observations can be made.

1. For security and privacy, the highest mean score at 4.22 represents a regular update of the applications leading to a secure method of transaction. The lowest score at 3.67 shows low levels of agreement among the customers about digital banking applications protecting their information online.
2. In case of trust, customers show the highest inclination with a score of 4.22 towards the presence of cybersecurity measures protecting their information online in banking transactions.
3. Majority of the customers agree that private sector banks provide an easy and quick management of the digital banking applications through innovative measures.
4. With a mean score of 4 for two items in the Awareness scale, the communication of private banks about online security is agreed by the majority of the customers.
5. Majority customers with a mean score of 4.33 agree that encryption of data is the best way to protect digital banking transaction data while having SMS or email alerts about monitoring has the lowest impact.
6. With a score of 4, the most challenging factors in terms of cybersecurity in banking include fraud calls, phishing, unauthorised access and viruses & malware.

The mean score analysis depicts a clear idea about the customers' perception on the security issues of the private bank's digital transactions.

In order to understand the impact of the challenging factors that occur in the cybersecurity activities of the digital banking sector on the security and privacy and trust of the customers, two regression models are constructed. Here, the challenging factors are termed as independent factors and the two factors of security and privacy and trust as dependent variables in the two models.

Table 2 - Model Fit Measures- Security & Privacy

				Overall Model Test			
Model	**R**	**R^2**	**Adjusted R^2**	**F**	**df1**	**df2**	**P**
1	**0.737**	**0.543**	**0.537**	**94.7**	**5**	**399**	**<.001**

Table 3- Model Coefficients - Security & Privacy

Predictor	**Estimate**	**SE**	**t**	**P**
Intercept	8.2976	0.2552	32.52	< .001
Un-updated information on the internet sources	-0.4606	0.0264	-17.4	< .001
Possibility of making fraud and scam calls.	-0.0465	0.0298	-1.56	0.120
Unauthorized access to the bank account.	-0.1535	0.0244	-6.29	< .001

Table 3- Model Coefficients - Security & Privacy				
Predictor	**Estimate**	**SE**	**t**	**P**
Down server of banks	-0.3676	0.0344	-10.6	< .001
Non-User-friendly interfaces of digital banking applications.	-0.0835	0.0334	-2.50	0.013
Malware and Viruses	-0.0485	0.0310	-1.68	0.129
Phishing	-0.0865	0.0364	-2.58	0.014

In case of security and privacy, it is seen that the regression model generated is statistically significant with a p-value of less than 0.05. The adjusted R^2 at 0.537 represents 53.7% variance caused by the independent factors on the levels of security and privacy about digital banking services in private banks. Now, moving into the coefficient table it is seen that out of the seven types of cybercrimes experienced, 5 have statistically significant impact on the dependent variable. It exerts a negative impact as can be seen from the estimates. This shows that one unit change in factors such as Un-updated information on the internet sources, making fraud and scam calls, Unauthorized access to the bank account, Non-User friendly interfaces of digital banking applications and phishing attacks can reduce the security and privacy perception levels of the private bank digital transaction among the customers by 53.7%. Hence, the private banks need to focus highly on reducing the challenges occurring in terms of these aspects to make the customers be confident about the security and privacy offered by the banks.

Table 4 - Model Fit Measures- Security & Privacy							
				Overall Model Test			
Model	**R**	**R^2**	**Adjusted R^2**	**F**	**df1**	**df2**	**P**
1	0.691	0.477	0.470	72.8	5	399	<.001

Table 5 - Model Coefficients – Trust				
Predictor	**Estimate**	**SE**	**t**	**P**
Intercept	7.0972	0.2614	27.15	< .001
Un-updated information on the internet sources	-0.4128	0.0270	-15.28	< .001
Possibility of making fraud and scam calls.	-0.1321	0.0305	-4.33	< .001
Unauthorized access to the bank account.	-0.0588	0.0250	-2.35	0.019
Down server of banks	-0.2849	0.0353	-8.07	< .001

Table 5 - Model Coefficients – Trust				
Predictor	**Estimate**	**SE**	**t**	**P**
Non-User-friendly interfaces of digital banking applications.	-0.0653	0.0342	1.91	0.057
Malware and Viruses	-0.0702	0.0449	2.05	0.061
Phishing	-0.0692	0.0356	1.92	0.055

In case of the perception about trust a similar pattern is observed among the customers. The adjusted R^2 in this case stands at 0.470 which is the level of variance explained by the independent factors. The further investigation shows that the first four challenges namely Un-updated information on the internet sources, making fraud and scam calls, Unauthorized access to the bank account and down server of banks impact on the trust levels of the customers about the security that the bank's digital banking methods are able to provide. Any unit change in these four items would vary the trust levels negatively in the customers by 47%.

It is evident that for both security & privacy and trust, the role of cybercrimes plays a significant role.

5. Conclusion

The role of technology and digitalisation on the entire world has been quite evident from the previous research conducted. The ways in which technology has been integrated across the different industries is quite fascinating to look into. One such industry which has experienced a total change in its mode of operations and providing services to its customers is the banking industry. The study here is an attempt to look into this mode of digital banking system as the advancement of online banking technology has changed people's lifestyles by becoming a part of their lives. Mobile phones are not just a medium of communication however, they became an information distribution platform and are used as computing devices. The traditional banking system is being replaced by mobile e-banking which is mostly preferred by a lot of the population. The evolution of individuals from the traditional to the digital banking phase has been limited by a number of issues. However, the prime focus when it comes to India is that of the cyber security issues that prevails all over. The previous literature paid more attention towards the adoption of digital banking among individuals with respect to the effectiveness and efficiency of the process. The Digital banking security aspect is less researched while it creates the majority of the problem in this regard. These studies are needed against fraudulent behaviour that govern such provisions. The lack of control over security makes Digital banking still untrusted for many customers till today because most of the customers are not informed about the privacy policies and even educated customers also do not maintain their privacy. Another side, Digital banking is a common target for hackers and other online criminals and the main reluctance customers are having while entering into online transactions is the security and

privacy issues. Commercial banks in India have been facing a lot of problems due to online banking crimes because they are dealing with personal property like personal data and passwords. These security issues have a direct impact on the intention to use digital banking methods and lead India towards a more technologically advanced nation in all forms. While other concerns of digital banking in India have been thoroughly discussed by researchers all over, this study would provide an in detailed idea into the impact caused by security issues.

The study here has been successful in highlighting the factors that influence the digital banking adoption. Future research can extend the study by adding more factors such as social media influence, peer pressure etc. in comprehending an overall outlook.

References

1. Aidonojie, P. A., Ikubanni, O. O., & Okuonghae, N. (2022). The Prospects, Challenges, and Legal Issues of Digital Banking in Nigeria. *14 Cogito: Multidisciplinary Res. J.*, *186*.
2. Dutta, D., & Sarma, M. K. (2021). An overview of the internet skills of digital platform users in a digitally emerging country: India. *International Journal of Trade and Global Markets*, *1*(1), 1. https://doi.org/10.1504/IJTGM.2021.10042600
3. Ghate, S., & Agrawal, P. K. (2017). A Literature Review on Cyber Security in Indian Context. *Journal of Computer & Information Technology*, *8*(05), 30–36. https://doi.org/10.22147/jucit/080501
4. Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis* (6th ed.). Pearson Prentice Hall.
5. Haryono, D., Saha Ghafur, A. H., & Rusliwa Somantri, G. (2023). The Challenges of Digital Banking in Today's Banking Industry. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, *6*(3), 2216–2234.
6. Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157–2177. https://doi.org/10.1007/s40747-021-00409-7
7. Jünger, M., & Mietzner, M. (2020). Banking goes digital: The adoption of FinTech services by German households. *Finance Research Letters*, *34*, 101260. https://doi.org/10.1016/j.frl.2019.08.008
8. Kaur, B., Kiran, S., Grima, S., & Rupeika-Apoga, R. (2021). Digital Banking in Northern India: The Risks on Customer Satisfaction. *Risks*, *9*(11), 209. https://doi.org/10.3390/risks9110209

9. Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society*, *64*, 101487. https://doi.org/10.1016/j.techsoc.2020.101487

10. Ngoc Thach, N., Thanh Hanh, H., Ngoc Huy, D. T., Gwozdziewicz, S., Viet Nga, L. T., & Thanh Huong, L. T. (2021). TECHNOLOGY QUALITY MANAGEMENT OF THE INDUSTRY 4.0 AND CYBERSECURITY RISK MANAGEMENT ON CURRENT BANKING ACTIVITIES IN EMERGING MARKETS - THE CASE IN VIETNAM. *International Journal for Quality Research*, *15*(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

11. Patnaik, A., Kudal, P., Dawar, S., Inamdar, V., & Dawar, P. (2023). Exploring User Acceptance of Digital Payments in India: An Empirical Study Using an Extended Technology Acceptance Model in the Fintech Landscape. *International Journal of Sustainable Development and Planning*, *18*(8), 2587–2597. https://doi.org/10.18280/ijsdp.180831

12. Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: an empirical analysis. *International Journal of Emerging Markets*, *18*(10), 4270–4300. https://doi.org/10.1108/IJOEM-06-2020-0724

13. Saxena, N., Gera, N., & Taneja, M. (2023). An empirical study on facilitators and inhibitors of adoption of mobile banking in India. *Electronic Commerce Research*, *23*(4), 2573–2604. https://doi.org/10.1007/s10660-022-09556-6

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