Journal of Posthumanism

2025
Volume: 5, No: 2, pp. 1079–1091
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i2.485

Analyzing the Effect of Cyber Security on FinTech Variables (Evidence from Jordanian Banks)

Nour Ali Nussir[1], Ali Ibrahim Abu Eid[2], Rasha Mohammad Rath'an Alraqqad[3], Emad Alsukhni[4], Saleh Mohammed Baqader[5], Mahmud Alataibi[6], Mohammad Hariri[7], Sultan Abdullah Alabdullatif[8], Ayman Hassan Bazhair[9], Ashraf Jahmani[10]

Abstract

The current study aiming at finding out the extent of awareness of the importance of cyber security among dealers using financial technology instruments and the role played by technology infrastructures. A questionnaire was employed to study this association. 370 questionnaires were issued to employees at three Jordanian banks, ranging from the frontline to the management level. It was shown that there is a statistically significant connection between the utilization of Fintech tools and cyber security.

Keywords: *Cyber Security, Financial Technology, Technology Infrastructure.*

Introduction

With the expansion of digital services and the emergence of electronic payment methods in addition to digital currencies and block chain, and the increasing importance of financial innovations at the level of the banking and financial sector **iqbal et al (2020)**, the need to create a security system to combat the penetration of personal accounts of customers, electronic hacking and information security risk management **Peters et al (2015)**. In response to this, in 2021 the Central Bank of Jordan developed a special program for information security in the banking sector under the name of Cyber Security at the level of the banking and financial sector, which aims to provide a secure banking environment at the highest level of confidentiality, The

[1] Assistant Professor, College of Business, Department of Finance and Banking Science, Jarash University, Jordan, Email: nnussir@jpu.edu.jo.
[2] Assistant Professor, College of Business, Department of Financial technology, Jadara University, Jordan, Irbid, Email: a.abueid@jadara.edu.jo.
[3] Assistant Professor, College of Business, Department of business administration, Jadara University, Jordan, Irbid, Email: r.alraqqad@jadara.edu.jo.
[4] Associate professor, IS department, Faculty of information technology and computer science Yarmouk University, Jordan, Irbid, Email: ealsukhni@yup.edu.jo.
[5] Associate professor, department of accounting, College of Business and Economics, Umm Al-Qura University, Makkah, Saudi Arabia, Email: smbaqader@uqu.edu.sa.
[6] Associate professor, Department of Financial Technology, Faculty of Economics and Administrative Sciences, Zarqa University, Zarqa, Jordan, Email: malataibi@zu.edu.jo.
[7] Associate professor, department of accounting, College of Business and Economics, Umm Al-Qura University, Makkah, Saudi Arabia, Email: mmharriri@uqu.edu.sa.
[8] Associate professor, department of accounting, College of Business and Economics, Umm Al-Qura University, Makkah, Saudi Arabia, Email: saabdullatif@uqu.edu.sa.
[9] Assistant Professor, Faculty of Business Administration, Department of Economics and Finance, Taif University, Taif, Saudi Arabia. Email abazhair@tu.edu.sa.
[10] Associate Professor, Faculty of Hospitality and Tourism Management, Al-Ahliyya Amman University, Email: ajahmani@ammanu.edu.jo.

Jordan Central Bank has also given directives to adapt to cyber risks to serve as a pillar in directing all banking sector institutions to the need to govern cyber security and manage cyber risks, so the Central Bank created at the beginning of 2021 a special unit to respond to cyber incidents for the financial and banking sector with the aim of enhancing the readiness and capacity of this sector Facing any potential risks in light of the trends towards relying on technology to provide digital financial services more in Jordan, such as the e-fawateercom system and jo mopay, where electronic payment settlements have become very popular among Jordanians, reaching nearly 14 billion JD during the last two years **Central Bank of Jordan(2021)**.

With the increase in electronic attacks around the world (as Jordan is not isolated from the rest of the world) and the increase in the risks surrounding financial transactions in the financial sector. According to **Magnuson (2018),** a number of variables, the most significant of which is the global financial system's unparalleled digital transition, which is being expedited by the COVID-19 pandemic, contributed to the worsening of these vulnerabilities. Banks and technology companies compete with one another. Meanwhile, the pandemic has raised the need for internet financial services. Global central banks are considering backing digital currencies and modernizing payment systems (Jam et al., 2011). Cybersecurity is more critical than ever at this time of change, when a single event may quickly erode trust and prevent such progress (Khan et al., 2016).

Second, malicious actors are taking advantage of this digital change, posing a growing threat to system integrity, financial stability, and public trust. Due to the pandemic, hackers now have new targets. According to the Bank for International Settlements IMF (2021), the financial industry is seeing the second-highest proportion of COVID-19-related cyberattacks, trailing only the health sector **Shahwan, Y. (2018)**.

Because of the significance of this study, which tries to evaluate the amount of knowledge of the value, effectiveness, and efficiency of cybersecurity controls in financial technology innovations in the banking sector, as well as the role of technical infrastructure in it, The study's key hypothesis can be stated as follows:

Cybersecurity has a significant effect on financial technology in Jordanian banks (α 0.05). a major hypothesis of the research can be formulated

To answer the study's difficulty and establish the validity of the hypothesis, the descriptive-analytical method will be employed with a survey created by the researchers.

Literature Review

Naviglia, James (2018) discussed the importance of cybersecurity and RegTech side by side and their impact on the stable and productive financial technology industry because of its impact on enhancing consumer confidence in electronic financial services. While **Adholiya & Adholiya (2019)** aimed in there study to measure the awareness of Udaipur Bank clients of the danger of cyber-security attacks and the threats surrounding their financial transactions in order to ensure measures to improve the level of awareness of cybersecurity procedures and advice to guarantee the security of their devices and digital activities. Meanwhile **Jayalath & Premaratne (2021)** discussed the impact of digital technology infrastructure and the necessary cybersecurity requirements on providing broad, fast, easy and uninterrupted banking services through financial channels by building a customer base via the Internet. **Al_Duhaidahawi et al (2020)** To gauge the influence of financial technology, the researchers sent out a questionnaire to people who

work in the technology sector in banks in Lebanon and Iraq with its four dimensions, Including self-efficacy, information security experiments, technological culture, and the competency and skills of these institutions' cybersecurity, as determined by financial risk management, banking, and financial services. **Sadekin & Shaikh (2016)** found that despite the facilities in electronic banking services that were provided by Bangladeshi banks, customers are not willing to use them due to their limited knowledge and lack of confidence in electronic banking services. **Khan & Malaika (2021)** In their paper they focused on the results obtained from the database of Article IV of the International Monetary Fund and highlighted the cyber security of central banks and the risks of financial technology and the mechanism for managing these risks through training employees and members of the board of directors and establishing a specialized department for risk management and linking it to the strategic planning of central banks. In terms of human resource development, Islamic Jordanian banks have significant challenges, such as rising staff turnover and a shortage of trained personnel. Insufficient research expenditures and poor performance management exacerbated these issues. **(Al-Fakeh, Padlee, Omar, & Salleh, 2020).**

Moses & Ogbuefi (2019) highlighted on the problems facing financial technology in Nigeria and South Africa, the most important of which are cybersecurity and electronic piracy, and proposing solutions to confront and reduce these problems**. Ismail (2019)** emphasized on the importance of the Arab supervisory bodies setting up a supervisory mechanism on the banking sector to ensure existence of controls and policies to achieve cyber security and work to enhance the degree of cybersecurity culture between customers by increasing customer awareness using multimedia programs and educational workshops in the financial and banking sector, with the aim of understanding the controls Instructions for the security of information systems and Cyber security. **Mani (2019)** recommended that spending should be made on managing cybersecurity risks just as spending is on developing financial technology tools and services because of its importance in gaining customers' confidence and reducing opportunities for cybersecurity risks . According to Najaf et al. (2020), the finance industry is 300 times more susceptible to computer counterfeiting than any other sector.., also found that after traditional banks in America cooperate with financial technology companies; they increase their exposure to cybersecurity risks. **Hamirani (2020)** focused on the need to frequently and routinely repair the web system to fix any security holes in a way that ensures its protection from any hacking or attacks, and employees must be trained on electronic fraud and remove all access privileges for any staff member who leaves the company. Employees are valuable assets to organizations because they are the ones that generate profits **(Alown, Al-Fakeh & Aburumman, 2021)**. **Kumar et al (2022)** The importance of their study came from that it is trying to understand the behavior of users of online banking services in order to identify their needs with regard to security and privacy, as they are the main factors that affect the adoption of the use of electronic banking services**. Iqbal et al (2020)** they suggested in order to support the effectiveness of cybersecurity, cooperation and alliance must be made, not only at the level of companies, industry and governments, but there must be a common culture around the world in order to achieve prosperity and stability by pushing away the risks of cybersecurity, which will help financial services companies to expand the spread of their services. **Selvaraj (2021)** reviewed the previous literature that dealt with the topic of cybersecurity and its impact on financial technology companies and also he discussed the most significant difficulties facing cybersecurity, such as the lack of awareness, system enhancement, Regulatory Challenges and cost.

Theoretical Framework

Of late, **Kumar et al (2022)** are trying to understand the behavior of users of online banking services in order to identify their needs with regard to security and privacy, **Hamirani (2020)** focused on the need to frequently and routinely repair the web system to fix any security holes in a way that ensures its protection from any hacking, According to a study by **Hamirani (2020),** the financial sector is 300 times more susceptible to cyberattacks than any other industry, which raises the stakes for cybersecurity concerns.

Based to the literature study and the reasoning above, the present framework of theory recommends that the dependent variable be financial technology (FINTECH), which may be evaluated by some of the supporting factors provided by confidence, security of information experiment, and Competence and skill, and technology culture and independent variable (Cybersecurity), While technology infrastructure was used as a mediating variable will have influence the using the Fintech instruments in Jordan, in other words The greater the awareness of the importance of cybersecurity, the greater the number of Fintech users. Thus,

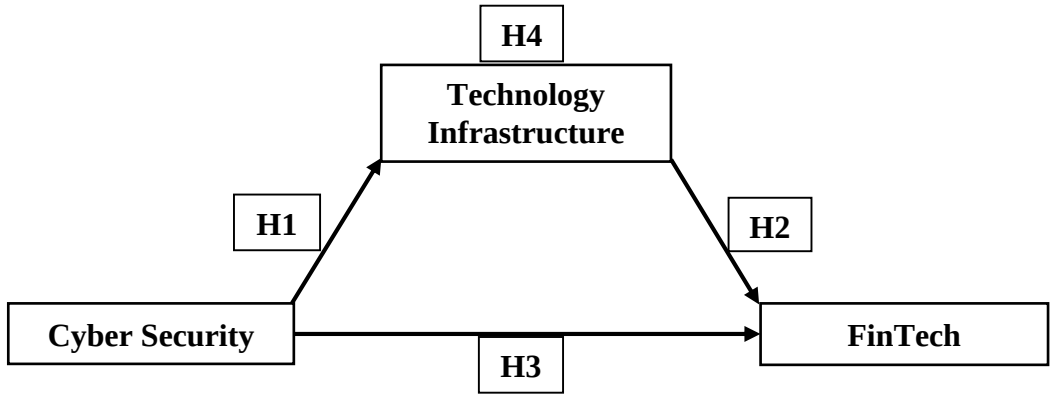

Figure 1: Proposed Model (prepared by researchers)

H1: Jordanian banks have a positive relationship with cyber security and technology infrastructure.

H2: Jordanian banks have a positive interaction with technology infrastructure and fintech.

H3: There is a good association between cyber security and fintech in Jordanian banking.

H4: Jordanian banks' technology infrastructure serves as a bridge between cyber security and fintech.

Methodology

Sample

In this study, we concentrated on objective measurements and statistical analysis of data collected through questionnaires, using quantitative methodologies and a probability sampling strategy to determine sample size. Quantitative research is concerned with acquiring quantitative data and using it in order to comprehend an instance or to apply it to a group of individuals.

Population & Data Collection

The intended audience for this essay consisted of 5400 personnel from the Bank of Jordan, Cairo Amman Bank, and Jordan Ahli Bank in the Hashemite Kingdom of Jordan. Furthermore, 357 respondents from the target group, representing all levels of bank employees from management.

Consequently, after delivering the questionnaires for this study, we used a self-administered approach to collect the respondents' questionnaire responses. Respondents have access to 370 questionnaires for scientific research. The researchers used a variety of tactics to increase the current study's response rate. First, questionnaires were distributed individually, accompanied with an introduction detailing the study's objectives. Then they assured participants that any data they submitted in the surveys was going to be kept completely secret. Additionally, the researchers employed a limited number of employees who served as each the financial institution's business sources. This team was in charge of acquiring surveys from various employees and persuading them to complete them. The final outcome of data collection produced 303 questionnaires that could be examined, representing an 81% legitimate response rate. **Babbie (1992)** states that 60% of the answers are good and 70% are very good." This is a very reasonable rate.

Data Analysis

SPSS software version 25 was employed for filtering and cleaning the data by removing outliers before performing a statistical assessment of the demographics that were supplied by those who took part and verifying the tools' accuracy and reliability. The results are then examined via a software application with an intuitive user interface to variance-based structural equation modeling (SEM) that employs an incomplete least-squares (PLS) route modeling method to evaluate the structural and measurement models of the research framework (testing hypothesis).

Measurement

The questionnaire was created with all of the components' measuring elements utilizing a scale of five stars that included (strongly agree 5, agree 4, neutral 3, disagree 2, significantly disagree 1).

Prior investigation was used to modify 17 items from the equipment associated with the three framework components. Based on the context of the research, the 17 items were separated into five for assessing cyber security (CS), which had been changed from **Akgunduz (2018)**, and six to assess technical institutions (TI), which had been adapted from Murray. Six Fintech-related articles were additionally cited; **with Omar et al. (2017)**.Table 1 describes where the objects came from.

Table 1: Measurement Items and Sources

Construct	Code	Item
Cyber Security (CS) Akgunduz and Eryilmaz, (2018)	CS1	Does your organization regularly perform cyber-security assessment exercise?
	CS2	Does your organization follow the security control measures such as those of confidentiality, integrity, authenticity and non-repudiation?
	CS3	Has the implemented security controls in your organization lead

		to technological efficacy, process efficacy, and organizational efficacy?
	CS4	Is the current model extensible for dealing with emerging cyberspaces (external deficiencies), that may lead to enhanced cybersecurity in your organization?
	CS5	Can the existing risk management framework incorporate system drawbacks (internal deficiencies) to upgrade the current cybersecurity level in your organization?
Fintech (F) Murray and Holmes, (2021)	F1	The bank has modern technical equipment.
	F2	The bank provides various modern services in various fields, such as electronic services.
	F3	The bank works with Fintech startups.
	F4	The bank is making changes to its operations and relying more on financial technology.
	F5	The bank relies on block chain technology (a decentralized digital ledger) to record transactions.
	F6	The bank has a cyber-security system for early detection of fraud.
Technology Infrastructures (TI) Omar, et al., (2017)	TI1	The bank has modern technical equipment.
	TI2	The bank uses advanced software.
	TI3	The bank has internal and external communication software and networks.
	TI4	The bank has a database.
	TI5	The bank provides electronic protection systems to secure its transactions.
	TI6	The bank has artificial intelligence applications that collect and analyze data.

Demographic profile

Table 2 shows the sample's socioeconomic features: Men completed 195 (or 64.3%) of the 303 questions, while women filled out 108 (or 35.6%). In addition, 180 (59.4%) of respondents were aged 26 to 35. According to their marital status, 43.8% of respondents were married. In addition, 12.2% of employees possessed a PhD, 18.4% had a master's degree, 64% had a bachelor's degree and 0.5% a diploma or certificate. Front-line workers received the highest responses (58.7%), followed by supervisors (15.1%) in managerial positions. The vast majority of respondents (47.1%) have five to 10 years of experience.

Table 2: Respondents Profile (n = 303)

Description	***Frequency***	***%***	***Description***	***Frequency***	***%***
Gender			***Position***		
Male.	195	64.3%	Manager.	21	0.06%
Female.	108	35.6%	Assistant manager.	20	0.06%
Age (years)			Supervisor.	46	15.1%
25 & below.	44	14.5%	Executive.	34	11.2%
(26 – 35).	180	59.4%	Frontline employee.	178	58.7%
(36 – 45).	43	14.1%	Others.	4	0.01%
(46 & above).	36	11.8%			

Marital status			***Experience (years)***		
Single.	120	39.6%	Less than 1.	8	0.02%
Married.	133	43.8%	(1– 5).	63	20.7%
Divorced/widowed.	50	16.5%	(5 – 10).	143	47.1%
Qualification			(11 – 15).	61	20.1%
Doctorate.	37	12.2%	(16 & above).	28	0.09%
Master degree.	56	18.4%			
Bachelor degree.	194	64%			
Diploma and less.	16	0.5%			

Results

To evaluate hypotheses and examine mediation and immediate consequences, the current research employed a quantitative strategy as well as using the partial the least-squares structure equation modeling (PLS-SEM) technique. The structure of the model has been evaluated in two steps in order to verify the validity as well as reliability of the proposed measuring scales: measuring frameworks and the structural model assessments.

Measurement model analysis

The SmartPLS app was used to evaluate the model's implicit variables and methods of measurement. To start, there are 303 surveys. The model of measurement (external model) was then utilized to determine the tools' reliability and validity **(Hair, Ringle, and Sarstedt, 2011)**. Validation is a tool's capacity to evaluate the concept it is intended to examine, whilst reliable is an instrument's stability in measuring the notion it is supposed to assess **(Sekaran & Bougie, 2016)**). The PLS measurement framework was examined for validity in both convergent and discriminant terms, in addition to reliability (internal consistency). The testing model has the following demands: **Tan, Ramayah, and Popa (2017),** as well as **Hair et al. (2017)**, state that the average variation of data extracting (AVE) and combination reliability (CR) values must be at least 0.7. Every item loaded value has to be greater than 0.7 or 0.6. **Hair et al. (2010), 2017.**

Convergent validation for reliability evaluation, in contrast, determines whether a product especially predicts the latent variables that it is expected to assess **(Urbach & Ahlemann, 2010; Tan et al., 2017),** while AVE examines the amount of the variation in a value that the framework demonstrates from its assessing indications, as well as the total effect of an error of the estimation **(Fornell & Larcker, 1981; Ringle et al. 2015; Tan et al. 2017**). Table 3 shows the most recent reliable and accurate measurement framework developed with SmartPLS version 3.3.2.

Table 3: Results of Reflective Measurements Model – A Summary

Constructs	**Indicators**	**Convergent validity**			**Internal consistency reliability**	
		Loading	**Rho_A**	**(AVE)**	**Composite reliability**	**Cronbach's alpha**
		>0.60	**>0.50**	**>0.50**	**0.70-0.90**	**0.60-0.90**
Cyber Security (CS)	CS2	0.865	0.906	0.706	0.905	0.865
	CS3	0.914				
	CS4	0.812				
	CS5	0.763				
Fintech (F)	F1	0.867	0.933	0.744	0.946	0.930

	F2	0.766				
	F3	0.857				
	F4	0.899				
	F5	0.890				
	F6	0.889				
Technology Infrastructures (TI)	TI1	0.771	0.900	0.611	0.904	0.875
	TI2	0.828				
	TI3	0.806				
	TI4	0.727				
	TI5	0.715				
	TI6	0.833				

Table 3 shows the outcomes of the evaluation of the the model's reliability and validity assessments. Table 3 reveals that each of the the other items had factor loadings more than 0.7, with the exception of one item (CS1) which had an inadequate factor loading. The results additionally demonstrate that all constructions had values for CR that ranged from 0.904 to 0.946, that were higher than the criterion of 0.7. This supports the validity of the estimation approach used in this investigation **(Hair et al., 2017)**. Furthermore, the measuring model's validity in both directions were examined. When AVE values above the required range of 0.5 (0.611 to 0.744), the indicators' validity as convergent was recognized.

The discriminant validity is established when an item outperforms other concepts on its own. As a result, researchers evaluated discrimination validity through a comparison of the square of the root for every concept's AVE value to the connections between the two components (**Fornell and Larcker, 1981; Barclay and Lloyd, 1996**). As a result, Table 4 reveals that each construction is more closely linked to itself than any other building. This means that all concepts match the criteria for discriminating validity and hence can be employed. As a result, the testing model can be said to be both accurate and reliable. This proved the device's legitimacy as well as the data's accuracy.

Table 4: Fornell-Larcker Criterion

Construct	***CS***	***F***	***TI***
Cyber Security	**0.840**		
Fintech	0.830	**0.862**	
Technology Infrastructures	0.828	0.847	**0.882**

The Heterotrait-Monotrait Ratio (HTMT) is a metric employed by SmartPLS to determine the discriminating reliability of models for measurement. This innovative approach investigates the selective accuracy of the latent variables of interest. In accordance with **Kline (2015)**, HTMT levels have to be lower than the minimal permissible level.Gold and Arvind Malhotra invented the HTMT, or 85, in 2001. However, the HTMT analysis's confidence interval does not include an average value of 1 for any of the variables **(Henseler, Ringle, & Sarstedt, 2015)**, indicating that the predictor is legitimate. Table 5 shows the HTMT criteria results; it is clear that every single value of the HTMT for the latent constructs contained in the the model's total variables varied from 0.878 to 0.890., falling short of the minimum acceptable value of 0.90 **(Franke & Sarstedt, 2019).** This finding revealed that each latent conception evaluation had perfect discrimination **(Henseler et al., 2015).**

Table 5: The HTMT Criterion

Variables	*CS*	*F*	*TI*
Cyber Security			
Fintech	0.878		
Technology Infrastructures	0.880	0.890	

Structural Model Analysis

The structural model contains of constructs, also known as latent variables, and the routes that connect between them. Figure 2 shows the structural model conceptually, beginning with (CS, F, and TI). The four hypotheses stated in the study define the course of the arrows that connect the constructions. Figure 2 represents the standard estimates for the research's structured model, illustrating the direct relationships between (CS and TI), (TI and F), and (CS and F), alongside TI's mediation role in the link between CS and F. To explain, the correlation coefficient, which is a measure of path values, which reflects the intensity of the relationship between any two structures, ranges from -1 to +1 (Hair et al., 2017).

According to **Ramayah, Cheah, Chuah, Ting, and Memon (2016)** the significant levels for 2-tailed tests: p 10% (1.64), p 5% (1.96), and p 1 (2.58); additionally, marketing researchers employed the significant level of p 5%, as is common. **Hair et al. (2017)** suggest applying bias-corrected bootstrap intervals of confidence (lower and upper limit) to determine whether a route coefficient is significant in statistical terms. According to **Hair et al. (2017)**, a path has a considerable impact when the confidence interval for the computed path coefficient does not include zero. Table 6 shows the results of this study's structural approach, which used a total of 5000 samples with bootstrap case replacements equal to the initial 303 data set.

Figure 2: Structural Model Results

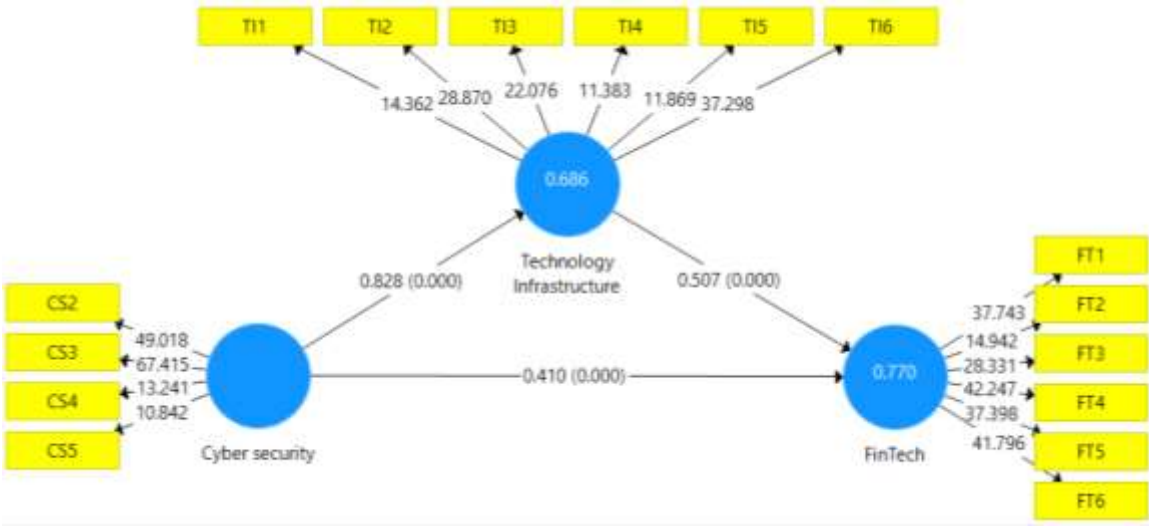

Table 6: Summary of the Structural Model Results

Hypothesis	Relationship	Indirect effect (β)	S. Error	t-Statistic	P Values	Confidence Interval (BC)		Decision
						LL	UL	
H1	Direct Relationship CS → TI	0.828	0.021	8.922	0.000	0.787	0.858	Supported*
H2	Direct Relationship TI → F	0.507	0.059	8.613	0.000	0.414	0.606	Supported*
H3	Direct Relationship CS → F	0.410	0.065	6.316	0.000	0.290	0.507	Supported*
H4	Indirect Relationship CS → TI → F	0.420	0.050	8.360	0.000	0.330	0.528	Supported*

Note: Significance level at *p < 0.01 (two-tailed). UL, upper limit at 95% confidence interval; LL, lower limit at 5%, BC, bias corrected.

In accordance with Table 6, the link between the route coefficients of CS and TI (direct effect) was discovered to be insignificant; the results indicated this (CS TI, =0.828; t-value of 8.922), indicating that H1 has been confirmed. The following hypothesis (H2) was statistically significant (p<0.01) showing agreement. The analysis found a strong correlation between CS and F (p<0.01), supporting H3.

The four hypotheses have been proposed for the current study, with CS serving as an independent variable and F as the dependent variable. TI acted as a bridge between them. The primary result of the study is that there is a statistically significant beneficial association among CS and TI. Additionally, research results show that TI mediators the relationship of CS and F.

Discussion

CS was the independent variable in this study, while the F was the dependent variable, leading to the development of four hypotheses. TI serves as a mediate variable between of them. The first finding or the study demonstrates that CS and technology infrastructure have a positive and statistically significant association, also, the results indicate that TI mediate the relationship between CS and F. This reveals that the sample of the study, represented by the three banks: Bank of Jordan, Cairo Amman Bank, and Jordan Ahli Bank, all of them possess good electronic protection systems to secure financial transactions and electronic services, which led to enhancing technological efficiency and effectiveness of the systems.

Conclusion

Financial technology is one of the methods created to facilitate human transactions and exchange of money, as it is characterized by flexibility, ease, and speed for users, but there are some threats that affect these transactions, such as information theft. Therefore, all aspects of cybersecurity must be taken into consideration during digital exchanges; FINTECH security is the protection of FINTCH assets from unauthorized access.

Recommendation

1. Conduct more practical analysis for companies about the elements of trust and security for customers and making sure that there are strategic plans to verify the existence of these two

elements and work on their development.

2. Financial institutions should not disclose any cyber-attacks they are exposed to and keep them private because of their role in undermining customer confidence.

3. Conduct longitudinal study either in Jordan or by extending it to different Arab country to counter the lack of generalization we are facing in this study.

Acknowledgement

This research was funded by Taif university, Saudi Arabia, Project No.(TU-DSPP-2024-228). The author extends his appreciation to Taif University, Saufi Arabia, for supporting this work through project number (TU-DSPP-2024-228).

References

Adholiya. A. Adholiya.S. (2019). A Study on Cyber Security Practices and Tips Awareness among E-Banking Services Users of Udaipur, Rajasthan, International Journal of Scientific Research in Multidisciplinary Studies, Vol.5, Issue.8, PP.148-154.

Al_Duhaidahawi, Hayder, Zhang, Jing, Abdulreza, Mustafa, Sebai, Meriem Harjan, Sinan. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks, International Journal of Research in Business and Social Science, Vol: 9, No: 6, PP: 123-133.

Al-Fakeh, F., Padlee, S., Omar, K., & Salleh, H. (2020). The moderating effects of organizational commitment on the relationship between employee satisfaction and employee performance in Jordanian Islamic banks. Management Science Letters, 10(14), 3347-3356.

Alown, B., Al-fakeh, F., & Aburumman, A. (2021). The role of quality of work life in Jordanian hotel industry. Management Science Letters, 11(2), 347-356.

Babbie E. (1992). The Practice of Social Research (6th Ed.). Wadsworth: Belmont, CA.

Barclay, L. M., & Lloyd, B. (1996). The misery of motherhood: alternative approaches to maternal distress. Midwifery, 12(3), 136-139.

Central Bank of Jordan. (2021). Cybersecurity Framework for Jordan Banking Sector, v1.0, PP1-145.

Fornell, C. & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research. 18(1), 39–50.

Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: a comparison of four procedures. Internet Research, 29(3), 430-447.

Gold, A. H., & Arvind Malhotra, A. H. S. (2001). Knowledge management: An organizational capabilities perspective. Journal of Management Information Systems, 18(1), 185-214.

Hair, J. F., Astrachan, C. B., Moisescu, O. I., Radomir, L., Sarstedt, M., Vaithilingam, S., & Ringle, C. M. (2021). Executing and interpreting applications of PLS-SEM: Updates for family business researchers. Journal of Family Business Strategy, 12(3), 100392.

Hair, J. F., Black, B., Babin, B., & Anderson, R. E. (2010). Multivariate Data Analysis. (7th ed.), Pearson Prentice Hall. Upper Saddle River, NJ.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed, a silver bullet. Journal of Marketing theory and Practice. 19(2), 139-152.

Hair, Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM). (2nd ed.), Sage publications, USA.

Hamirani, Ekbal. (2020). the Challenges for Cyber Security in E-Commerce, Conference Paper. PP: 1-6.

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.

Iqbal, Hena,Ul-Taibi, Ghassan, Pohra, Om Prakash. (2020).The Reality of Technologies for Cyber Security Challenges, International Journal of Recent Technology and Engineering, Vol -9, No-1, PP1-7.

Ismail, Mohammed. (2019). Cyber security in the banking sector, Arab Monetary Fund, Vol.4, P 1-8.

Jam, F. A., Khan, T. I., Zaidi, B., & Muzaffar, S. M. (2011). Political skills moderates the relationship between perception of organizational politics and job outcomes. Journal of Educational and Social Research, 1(4), 57-70.

Jayalath, J A R C, Premaratne, S. C. (2021). Analysis of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies, IJRP 2021, 84(1), 128-135.

Khan, Ashraf, Malaika, Majid. (2021). Central Bank Risk Management, Fintech, and Cybersecurity, International Monetary Fund Working Paper, PP: 1-76.

Khan, T. I., Akbar, A., Jam, F. A., & Saeed, M. M. (2016). A time-lagged study of the relationship between big five personality and ethical ideology. Ethics & Behavior, 26(6), 488-506.

Kline, R. B. (2015). Principles and practice of structural equation modeling. (4th ed.), Guilford publications, New York.

Kumar, Atul, Tiwari, Anubhav, Mantri, Jai, Chakraborty, Debanku. (2022). Study of Customer Aspects of Cyber Securities in E-Banking, Global Educational Leadership, Vol: 1, No.1, PP: 86-97.

Magnuson, W. (2018). Regulating fintech. Vanderbilt Law Review, Available at: https://scholarship.law.vanderbilt.edu/vlr/vol71/iss4/271 (4), 1167–1226.

Mani, Vimal. (2019). Cybersecurity and Fintech at a Crossroads, ISACA Journal, Vol. 2, PP .1-7.

Maurer, Tim and Nelson, Arthur. (2021). the Globale Cyber Threats, Finance & Development, International Monetary of Fund, PP: 24-27.

Moses, Faya, Ogbuefi, Nnubia. (2019). Cyber Secure Nigeria2019, Conference, Electronic copy available at: https://ssrn.com/abstract=3606866

Najaf, Khakan, Schinckus, Christophe, Mostafiz, Md Imtiaz, Najaf, Rabia. (2020). Conceptualising cybersecurity risk of fintech firms and banks sustainability, The International Conference on Business and Technology,Istanbul, Turkey, PP. 14-15.

Naviglia, Jennifer. James, Jason. (2018). FINTECH, REGTECH and the Importance of Cybersecurity, Issues in Information Systems, Volume 19, Issue 3, pp. 220-225.

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. SSRN Electronic Journal, 3(3). https://doi.org/10.2139/ssrn.2646618

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2016). Partial least squares structural equation modeling (PLS-SEM) using SmartPLS 3.0: An updated and practical guide to statistical analysis.

Ringle, C., Da Silva, D., & Bido, D. (2015). Structural equation modeling with the SmartPLS.

Sadekin, Mohammad, Shaikh, Md. (2016), Security of E-Banking in Bangladesh, Journal of Finance and Accounting, Vol. 4, No. 1, PP: 1-8.

Sekaran, U. (2003). Research methods for business: A skill building approach (4th Ed.), John Wiley & Sons, New York.

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.

Selvaraj, Nagasundari. (2021). The Essence of Cyber security Through Fintech 3.5 in Preventing and Detecting Financial Fraud: A Literature Review, Electronic Journal of Business and Management, Vol.6, No. 2, pp. 18-29.

Shahwan, Y. (2018). The mediating effect of investment decisions and financing decisions on the influence of capital structure against corporate performance: Evidence from Jordanian listed commercial banks.

Academy of accounting and Financial Studies journal, 22(6), 1-20.

Tan, C. N. L., Ramayah, T., & Popa, S. (2017). KMS self-efficacy, KMS quality, expected reward and subjective norm: investigating knowledge sharing attitude of Malaysia's Halal industry. European Journal of International Management, 11(4), 407-429.

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. Journal of Information technology theory and application. 11(2), 5-40.