JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
ICASET
2024

Research Article
Collection: Intelligent Computing of Applied Sciences and Emerging Trends

Impact of Cyber Security Measures in the Digital Banking Sector of Pakistan

Faisal Iqbal[1*], Syed Ali Nawaz[2], Rizwan Ali Shah[3], Muzammil-ur-Rehman[3], Asad Mushtaq Gujjar[4], Abhia Ejaz[3], Zeeshan Dilbar[3], and Tanveer Aslam[3]

[1]Internal Audit, U Microfinace Bank Ltd, Islamabad, 44080, Pakistan.
[2]Department of Information Technology, Islamia University of Bahawalpur, Bahawalpur Punjab, Pakistan.
[3]Department of Computer Science, Islamia University of Bahawalpur, Bahawalpur Punjab, Pakistan.
[4]Operations Department, Faysal Bank Limited, Karachi, Pakistan.
[*]Corresponding Author. Faisal Iqbal. Email: faisaliqbaal@gmail.com

Academic Editor: Salman Qadri **Published:** April 01, 2024

Abstract: The research aimed to investigate the traceability, vulnerability, and quality of the security risk framework, as well as the implementation and monitoring of security controls within a banking system. This inquiry sought to assess their impact on the performance of digital banking services offered by banking firms in the Pakistani banking industry. Employing a quantitative research approach, the study utilized primary data for analysis. The explanatory research procedure was chosen, focusing on mobile banking users with over one year of experience in electronic banking and a literacy level equal to or above matriculation. Convenience sampling was employed with a sample size of 138 participants. Data was collected through a questionnaire and analyzed using structural equation modeling with PLS smart software. The study revealed that the implementation of security controls had an insignificant impact on digital banking services performance (p-value = 0.228, > 0.05, rejecting H1). However, monitoring of security controls (p-value = 0.002, < 0.05, accepting H2), traceability (p-value = 0.019, < 0.05, accepting H4), and vulnerability (p-value = 0.011, < 0.05, accepting H5) significantly influenced digital banking services performance. All accepted hypotheses exhibited positive coefficients, indicating a constructive influence on the determination of digital banking services performance.

Keywords: Traceability; Vulnerability; Security Risk Framework; Implementations of Security Control; Monitoring of Security Control; Digital Banking Services Performance.

1. Introduction

Internet banking has revolutionized financial practices, providing customers and the banking sector with a 24/7 solution and cost-effective operations [1]. The shift to internet and mobile banking has transformed transactional dealings and facilitated the growth of electronic commerce, online businesses, and cashless practices [2]. Digital banking practices play a pivotal role in real-time facilitation for customers and corporations, boosting online business activities. Additionally, digital banking has promoted innovative cross-border practices with communication modes [3]. Ensuring security and privacy remains a vital concern in digital banking practices [4].

Research has extensively explored various dimensions of digital banking practices, discussing factors both constructively and restrictively affecting their promotion [5]. The use of secure communication protocols and addressing information transfer in end-to-end computing environments is crucial for maintaining end-to-end transaction security [6]. Financial institutions employ software-based systems with customized hardware for effective security control, using encryption algorithms, private and public keys, and digital signatures for secure electronic transactions [7]. The global trend in business practices has witnessed an increase in electronic commerce, with the banking industry adopting new communication methods

known as electronic banking systems [8]. Banking industry globally is in process of use of new communication methods to provide to customers with value added services a convenience. This phenomenon is generally called as electronic banking system [8].

2. Related Work

Despite the expansion of 4G technology in South Asian countries, the affordability of broadband internet and smartphones remains a challenge for a significant portion of the population. The region presents potential for digital business expansion, requiring regulatory support and infrastructure development [2].

Digital banking practices play a pivotal role in real-time facilitation for customers and corporations, boosting online business activities. Additionally, digital banking has promoted innovative cross-border practices with communication modes. Enhancing cybersecurity and protection is imperative for fostering a secure environment, increasing digital banking acceptance, and ensuring data privacy [3].

The South Asian region, including Pakistan, faces cyber threats, and there is a need for global efforts to address the disruptive cross-border phenomenon of cybersecurity. Cybersecurity controls, risk management policies, and standard operating procedures are essential for protecting against potential cyber threats in the banking sector [4].

Studies emphasize the positive correlation between cybersecurity effectiveness and digital confidence among customers, emphasizing the need for effective cross-border connectivity, improved data infrastructure, and protected cross-border data flows and payment activities. The COVID-19 pandemic has seen a 600% increase in cybercrimes, with an estimated annual cost of $10.5 trillion by 2025, emphasizing the urgency of sophisticated cybersecurity architecture [5].

The breach of cyber security is observed usually through skimming, phishing, pharming etc. The outcomes of cyber-security are commonly observed in the form of loss of reputation of financial institution, lack of systematic implications, vulnerability of cross-border and national payment or settlements along with pose of contagion risk to financial system. The Far East and China lead in active online banking users, with around 805 million users and an estimated growth to over 1 billion by 2024 [9].

The digital-only banks market size is projected to reach $2.05 trillion by 2030 from $47.4 billion in 2021. The electronic banking later on harmonized the ground for speedy and convenient banking services for both commercial entities and individuals [10].

In conclusion, cybersecurity plays a crucial role in the sustainable future of banking firms, and this study focuses on e-banking security in Pakistan as a determinant of confidence and the future of e-banking services in the country.

3. Materials and Methods

The current research employed a questionnaire as the primary data collection instrument, chosen based on the nature of the data under consideration. Utilizing a questionnaire proved to be an efficient method for analysis, enabling the collection of responses from a large number of participants with limited resources. The questionnaire consisted of carefully selected questions from prior investigations, incorporating a Likert scale ranging from 1 to 5 (1 for strongly disagree, 2 for disagree, 3 for neutral, 4 for agree, and 5 for strongly agree). This scale facilitated the capture of a diverse range of responses, allowing for a comprehensive analysis of variations. The survey-based approach was adopted for response collection, utilizing platforms such as Google Forms, email correspondence, telephonic communication, social media, and physical response collection. This multi-channel approach was instrumental in obtaining the necessary volume of responses within the specified time constraints.

The research model of the present research based investigation has been mentioned below.

$$DBSP = \beta_0 + \beta_1 TRA + \beta_2 VUL + \beta_3 SRF + \beta_4 ISC + \beta_5 MSC + Error\ Term$$

Where,

TRA = Traceability

VUL = Vulnerability

SRF = Security Risk Framework

ISC = Implementations of Security Control

MSC = Monitoring of Security Control

DBSP = Digital Banking Services Performance

3.1. Research Model

Over cyber security and performance evaluation framework is initiated by first of all identified all population in the next step data is gathered, and we select our dataset to process further. The parameter of the research model are specified and statistical processing is applied on the model. The overall framework of Cyber security measure and banking performance evaluation is given in the Figure 1.

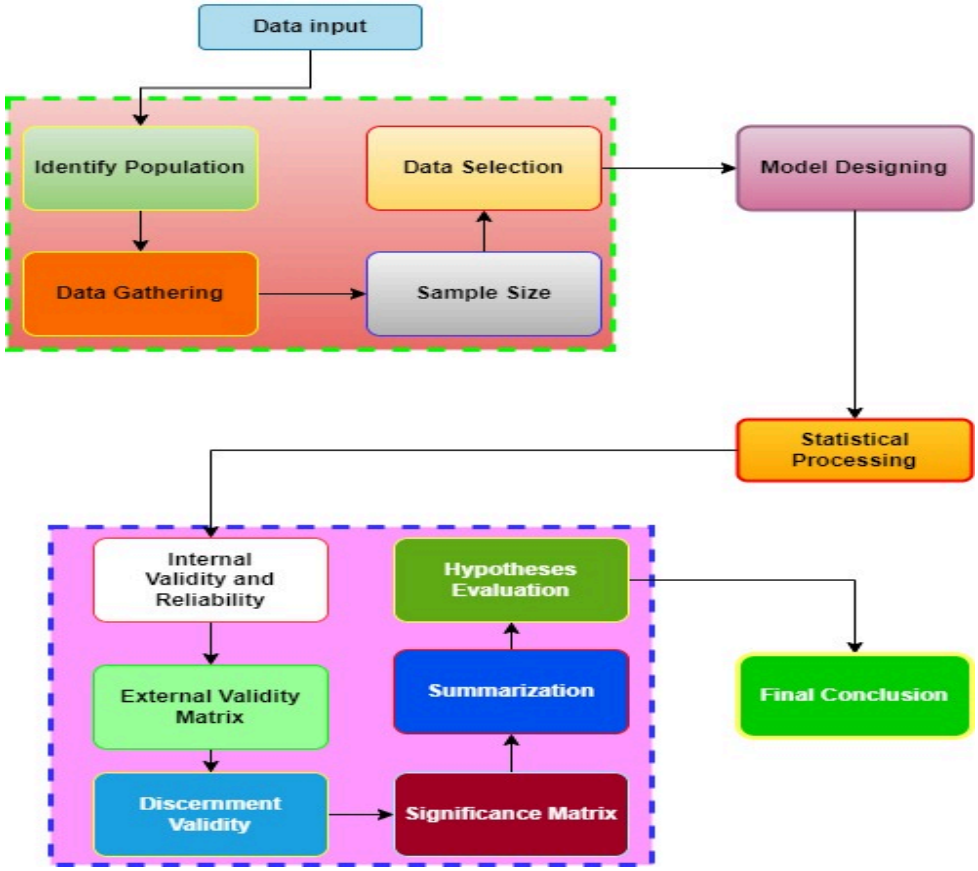

Figure 1. Research Model

The current research study involves the analysis of the primary collected responses through descriptive statistics. Descriptive statistics are employed to evaluate mean values, standard deviation, kurtosis, and skewness of the responses. Additionally, demographic information is utilized to create a frequency distribution, providing insights into the characteristics of the respondents. The analysis proceeds with reliability and validity tests at a 5 percent significance level, including an assessment of multi-collinearity and autocorrelation. Finally, a regression method is applied to the data to determine the overall significance of the model at a 5 percent level, extracting coefficient values to examine each independent variable and conducting hypotheses testing. This comprehensive analysis is conducted using PLS Smart and the application of structural equation modeling.

3.2. Dataset Collection

The present study has selected questionnaire as data collection instrument as present study considered with the use based on the nature of data selected for the current study. The present study selected with the survey-based approach to collect with responses. The option includes with the google form, email-based communication, telephonic communication, social media, and physical response collection. Electronic banking system make use of banking data for initiation of transactions with other banks or with other financial services providers in a remote manner using telecommunication mechanism. The is greater share of online banking users in Far East and China followed by rest of the world, Europe, North America, and Latin America as mentioned below in Figure 2.

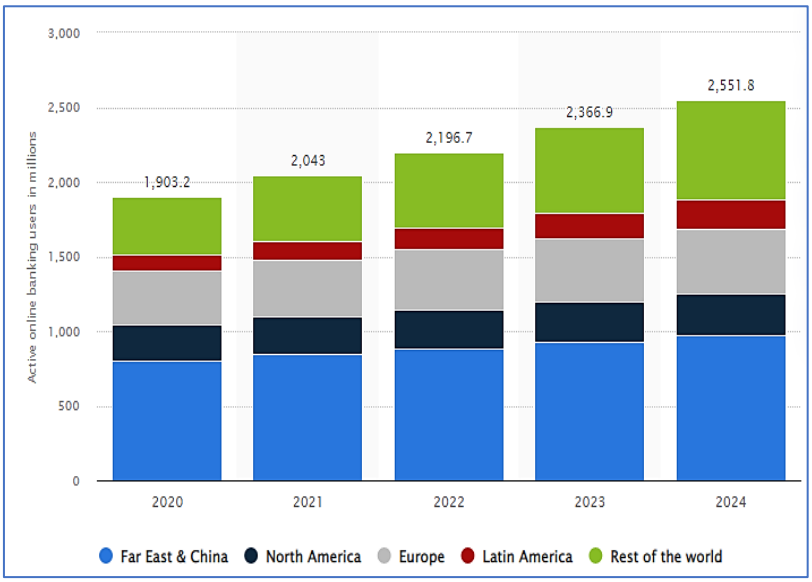

Figure 2. No. of Active Online Banking Users

4. Experiments and Results

It is followed with testing of constructed hypotheses and interpretation of coefficient values. At last hypotheses summary has been described.

4.1. Outer Loading Value

The value of outer loading should be greater than 0.7 to input its role in determination of the latent variable and the same has been used as a selection criterion of the item. The value of outer loadings for items of traceability like TRAC1, TRAC2, TRAC3, TRAC4 and TRAC5 observed with 0.849, 0.774, 0.840, 0.889 and 0.847 respectively. All the values found higher than the 0.7 hence items have been retained within the model. The value of outer loadings for items of vulnerability like VULN1, VULN2, VULN3, VULN4 and VULN5 observed with 0.845, 0.729, 0.887, 0.890 and 0.883 respectively. All the values found higher than the 0.7 hence items have been retained within the model. The value of outer loadings for items of security risk framework like SCRF1, SCRF2, SCRF3, SCRF4 and SCRF5 observed with 0.918, 0.778, 0.857, 0.909 and 0.825 respectively. All the values found higher than the 0.7 hence items have been retained within the model.

The value of outer loadings for items of implementation of security controls like IOSC1, IOSC2, IOSC3, IOSC4 and IOSC5 observed with 0.840, 0.738, 0.882, 0.894 and 0.880 respectively. All the values found higher than the 0.7 hence items have been retained within the model. The value of outer loadings for items of monitoring of security control like MOSC1, MOSC2, MOSC3, MOSC4 and MOSC5 observed with 0.919, 0.760, 0.860, 0.897 and 0.827 respectively.

All the values found higher than the 0.7 hence items have been retained within the model. The value of outer loadings for items of digital banking services performance like DBSP1, DBSP2, DBSP3, DBSP4 and DBSP5 observed with 0.968, 0.942, 0.966, 0.946 and 0.971 respectively. All the values found higher than the 0.7 hence items have been retained within the model, which is described in Figure 3.

4.2. Internal Validity and Reliability

The above interpretation clearly revealed that all the outer loading values are higher than the 0.7 hence accepted and retained within the model. As also mentioned within Table 1. Furthermore, Cronbach's Alpha value was observed with a benchmark value of 0.7 and for the current study the value also observed higher than the 0.7 as mentioned below. The value of the reliability of Cronbach's Alpha of digital banking services performance, implementation of security controls, monitoring of security controls, security risk framework, traceability and vulnerability observed with value of 0.9779, 0.9031, 0.9084, 0.9109, 0.8959 and 0.9033 respectively. All the values observed were higher than the 0.7 hence got with satisfactory information regarding reliability. Furthermore, the value of the Rho A was also observed in acceptance range i.e. higher than the 0.7.

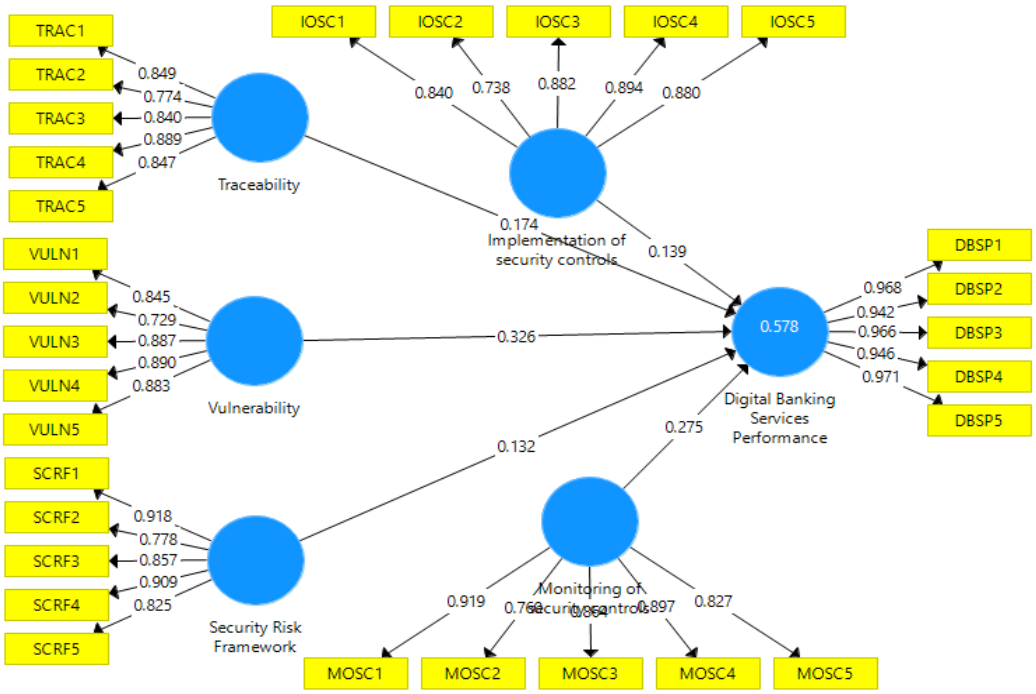

Figure 3. Outer Loading Values of Measured Model

The value of the reliability of Rho A of digital banking services performance, implementation of security controls, monitoring of security controls, security risk framework, traceability and vulnerability observed with value of 0.9782, 0.9227, 0.9349, 0.9307, 0.9066 and 0.9251 respectively. All the values observed were higher than the 0.7 hence got satisfactory information regarding reliability. Furthermore, the value of the Rho A is also observed in acceptance range i.e. higher than the 0.7, which is shown in Table 1.

Another measure of the internal reliability is the composite reliability that is validity of the internal reliability in addition to Cronbach's Alpha and Rho A. The value of the composite reliability should be higher than the values of Cronbach's Alpha and Rho A. The value of composite reliability of digital banking services performance, implementation of security controls, monitoring of security controls, security risk framework, traceability and vulnerability observed with 0.9827, 0.9277, 0.9314, 0.9333, 0.9232 and 0.9278 respectively. All the values observed were higher than 0.7. All three tests of internal reliability reported satisfactory values and accepted for the study. At last, the average variance extracted value for internal validity reported with the value of 0.9191, 0.7206, 0.7316, 0.7375, 0.7067 and 0.7209 respectively. All the values of the internal validity reported with the value higher than the 0.5 and accepted with the internal validity.

Table1. Internal Validity and Reliability

Latent Variables	Items	Outer Loadings	Cronbach's Alpha	Rho A	Composite Reliability	Average Variance Extracted (AVE)
Digital Banking Services Performance	DBSP1	0.9678	0.9779	0.9782	0.9827	0.9191
	DBSP2	0.9420				
	DBSP3	0.9656				
	DBSP4	0.9463				
	DBSP5	0.9714				
Implementation of security controls	IOSC1	0.8402	0.9031	0.9227	0.9277	0.7206
	IOSC2	0.7380				
	IOSC3	0.8820				
	IOSC4	0.8942				
	IOSC5	0.8802				

Monitoring of security controls	MOSC1	0.9191	0.9084	0.9349	0.9314	0.7316
	MOSC2	0.7600				
	MOSC3	0.8642				
	MOSC4	0.8970				
	MOSC5	0.8272				
Security Risk Framework	SCRF1	0.9179	0.9109	0.9307	0.9333	0.7375
	SCRF2	0.7780				
	SCRF3	0.8568				
	SCRF4	0.9088				
	SCRF5	0.8246				
Traceability	TRAC1	0.8486	0.8959	0.9066	0.9232	0.7067
	TRAC2	0.7741				
	TRAC3	0.8400				
	TRAC4	0.8891				
	TRAC5	0.8473				
Vulnerability	VULN1	0.8449	0.9033	0.9251	0.9278	0.7209
	VULN2	0.7290				
	VULN3	0.8870				
	VULN4	0.8901				
	VULN5	0.8833				

The path coefficient values of the below table shows that the p-value of implementation of security controls on digital banking services performance observed 0.228 i.e. higher than the 0.05 hence found insignificant and got with rejection of H1. The path coefficient values of the below table shows that the p-value of monitoring of security controls on digital banking services performance observed 0.002 i.e. lower than the 0.05 hence found significant and got with acceptance of H2. The path coefficient values of the below table shows that the p-value of security risk framework on digital banking services performance observed 0.160 i.e. higher than the 0.05 hence found insignificant and got with rejection of H3.

The path coefficient values of the below table shows that the p-value of traceability on digital banking services performance observed 0.019 i.e. lower than the 0.05 hence found significant and got with acceptance of H4. The path coefficient values of the below table shows that the p-value of vulnerability on digital banking services performance observed 0.011 i.e. lower than the 0.05 hence found significant and got with acceptance of H5. All the coefficient values of the accepted hypotheses observed positive in nature hence found determination of digital banking services performance constructively. Traceability -> digital banking services performance. All output dataset in Table 2.

Table 2. Path Coefficient & Hypotheses Testing

	Original Sample (O)	**Sample Mean (M)**	**Standard Deviation (STDEV)**	**T Statistics (|O/STDEV|)**	**P Values**
H1: Implementation of security controls -> Digital Banking Services Performance	0.139	0.128	0.115	1.207	0.228
H2: Monitoring of security controls -> Digital Banking Services Performance	0.275	0.269	0.090	3.061	0.002
H3: Security Risk Framework -> Digital Banking Services Performance	0.132	0.139	0.094	1.407	0.160
H4: Traceability -> Digital Banking Services Performance	0.174	0.182	0.074	2.363	0.019
H5: Vulnerability -> Digital Banking Services Performance	0.326	0.328	0.128	2.543	0.011

4.3. Hypotheses Summary

Out determined hypotheses are H1, H2, H3, H4, and H5. Every hypothesis has been tested on the significant value. The complete summary of the tested hypotheses has been mentioned below in Table 3.

Table 3. Hypotheses Summary

Sr.	Hypotheses	Sig. Value	Comments
1	H1: There is significant impact of traceability of electronic cyber security of a banking system in determination of banking firm's digital banking services performance.	0.019	Hypotheses accepted
2	H2: There is significant impact of vulnerability of electronic cyber security of a banking system in determination of banking firm's digital banking services performance.	0.011	Hypotheses accepted
3	H3: There is significant impact of security risk framework of a banking system in determination of banking firm's digital banking services performance.	0.160	Hypotheses rejected
4	H4: There is significant impact of implementation of security controls of a banking system in determination of banking firm's digital banking services performance.	0.228	Hypotheses rejected
5	H5: There is significant impact of monitoring of security controls of a banking system in determination of banking firm's digital banking services performance.	0.002	Hypotheses accepted

5. Discussion

The present study clearly revealed that there is a significant impact of traceability of electronic cyber security of a banking system in determination of banking firm's digital banking services performance. The is because traceability of electronic cyber security of a banking system reveals with its strength in monitoring of operations hence found with positive relationship [11] observed with significant impact on the performance of services offered to customer along with element of trust on services. Another study also revealed with an investigation of cybercriminal incidences linked with the online banking activities [13]. The study found with application of two factor authentication feasibility of traceability[12]. The study also revealed with the weakness of the user-friendly measures as weak factor to the security framework along with its increased vulnerability to exploitation online banking services [14]. Another study also investigated the risk factors associated to the intention of the customers to retain with the electronic banking services. The study observed with the presence of opportunity cost risk, loss risk, traceability and opportunity cost risk that ultimately affect the usefulness of the internet banking services and its usage among customers. Electronic banking observed with positive increase in use with an improved level of traceability with consideration of cybersecurity risk factors [15].

6. Conclusions

This study investigated with the traceability and vulnerability of electronic cyber security, quality of security risk framework of a banking system, implementation of security controls and monitoring of security controls of a banking system in determination of banking firm's digital banking services performance in case of Pakistan banking industry. The study based on the quantitative research approach. The study used with the primary data as there is no published source of information i.e. secondary data, to conduct the current investigation. The study selected with the explanatory research procedure to determine the impact of traceability, vulnerability, security risk framework, implementation of security measures and control on digital banking service performance in Pakistan from technology perspective.

The targeted population selected for the current study are mobile banking users having more than 1-year experience of using electronic banking services along with literacy level above or equal to matriculation. The current study has selected with the convenience sampling technique. the current study selected with a sample size of 138. The present study selected questionnaire as data collection instrument as present study. The collected data has applied with the structural equation modeling using PLS smart as software. The results of the study revealed that the p-value of implementation of security controls on digital banking

services performance observed 0.228 i.e. higher than the 0.05 hence found insignificant and got with rejection of H1. The p-value of monitoring of security controls on digital banking services performance observed 0.002 i.e. lower than the 0.05 hence found significant and got with acceptance of H2.

The p-value of security risk framework on digital banking services performance observed 0.160 i.e. higher than the 0.05 hence found insignificant and got with rejection of H3. The path coefficient values of the below table shows that the p-value of traceability on digital banking services performance observed 0.019 i.e. lower than the 0.05 hence found significant and got with acceptance of H4. The path coefficient values of the below table shows that the p-value of vulnerability on digital banking services performance observed 0.011 i.e. lower than the 0.05 hence found significant and got with acceptance of H5. All the coefficient values of the accepted hypotheses observed positive in nature hence found determination of digital banking services performance constructively.

References

1. I. Koskosas, "E-banking security: A communication perspective," Risk Manag., vol. 13, pp. 81–99, Feb. 2011, doi: 10.2307/41289358.
2. A. O. Alsayed and A. Bilgrami, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities International Journal of Emerging Technology and Advanced Engineering E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention," Int. J. Emerg. Technol. Adv. Eng., vol. 7, no. 1, pp. 109–115, 2008, [Online]. Available: https://www.researchgate.net/publication/315399380
3. C. Belbergui, N. EL KAMOUN, and H. Rachid, "E-banking Overview: Concepts, Challenges and Solutions," Wirel. Pers. Commun., vol. 117, pp. 1–20, Mar. 2021, doi: 10.1007/s11277-020-07911-0.
4. N. Mehmood, F. Shah, M. F. Azhar, and A. Rasheed, "The Factors Effecting E-banking Usage in Pakistan," 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:55112313
5. I. Haq and T. Awan, "Impact of e-banking service quality on e-loyalty in pandemic times through interplay of e-satisfaction," Vilakshan - XIMB J. Manag., vol. ahead-of-print, Oct. 2020, doi: 10.1108/XJM-07-2020-0039.
6. I. Ahmad, S. Iqbal, S. Jamil, and M. Kamran, "A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques," Linguist. Antverp., vol. 2021, pp. 3509–3517, Jun. 2021.
7. M. Kumar and S. Gupta, "Security perception of e-banking users in India: An analytical hierarchy process," Banks Bank Syst., vol. 15, no. 1, pp. 11–20, 2020, doi: 10.21511/bbs.15(1).2020.02.
8. S. Sandhu and S. Arora, "Customers' usage behaviour of e-banking services: Interplay of electronic banking and traditional banking," Int. J. Financ. Econ., vol. 27, Oct. 2020, doi: 10.1002/ijfe.2266.
9. T. Hassan and Ahamd, Transaction and Identity Authentication Security Model for E-Banking: Confluence of Quantum Cryptography and AI | SpringerLink Transaction and Identity Authentication Security Model for E-Banking: Confluence of Quantum Cryptography and AI International Conference on Intelligent Technologies and Applications INTAP 2018: Intelligent Technologies and Applications pp 338-347 | Cite as. 2019.
10. K. Al Omoush, M. Al Attar, I. Saleh, and A. Alsmadi, "The drivers of E-banking entrepreneurship: an empirical study," Int. J. Bank Mark., vol. ahead-of-print, Oct. 2019, doi: 10.1108/IJBM-03-2019-0113.
11. S. Demirkan, I. Demirkan, and A. Mckee, "Blockchain technology in the future of business cyber security," Feb. 2020, doi: 10.1080/23270012.2020.1731721.
12. N. Kassim and T. Ramayah, "Perceived Risk Factors Influence on Intention to Continue Using Internet Banking among Malaysians," Glob. Bus. Rev., vol. 16, pp. 393–414, Jun. 2015, doi: 10.1177/0972150915569928.
13. S. A. Nawaz, D. M. Khan, and S. Qadri, "Brain Tumor Classification Based on Hybrid Optimized Multi-features Analysis Using Magnetic Resonance Imaging Dataset," Applied Artificial Intelligence, vol. 36, no. 1, 2022, doi: 10.1080/08839514.2022.2031824.
14. A. F. M. Shahen Shah et al., "On the Vital Aspects and Characteristics of Cryptocurrency—A Survey," IEEE Access, vol. 11, pp. 9451–9468, 2023, doi: 10.1109/ACCESS.2023.3240103.
15. W. Elmasry, A. Akbulut, and A. H. Zaim, "Empirical study on multiclass classification-based network intrusion detection," Comput Intell, vol. 35, no. 4, pp. 919–954, Nov. 2019, doi: 10.1111/COIN.12220.