European Economic Letters
ISSN 2323-5233
Vol 14, Issue 4 (2024)
http://eelet.org.uk

"A Study on the Customer Awareness on Security Issues and Threats in Digital Banking in Chennai"

Dr. Sankararaman G[1], Dr. Suresh S[2], Dr Thirumagal PG[3], Priyadharshini V[4] and Dr. Rengarajan V[5]

1. Professor in Management Studies, Rajalakshmi Engineering College, Chennai
2. Associate Professor in Management Studies, Rajalakshmi Engineering College, Chennai
3. Professor and Head, School of Management Studies, VISTAS University, Chennai
4. Student of Management Studies, Rajalakshmi Engineering College, Chennai
Senior Assistant Professor, School of Management Studies, SASTRA University, Thanjavur

ABSTRACT

Digital banking has revolutionized the way financial transactions are conducted, offering convenience and accessibility like never before. However, this paradigm shift also brings forth a myriad of security threats and challenges. This paper aims to evaluate the overall awareness level among customers regarding security threats and issues in digital banking. Through a comprehensive study, the specific digital banking security threats that customers are most aware of will be identified. Additionally, customers' understanding of security protocols and best practices while using net banking services will be assessed, along with determining the extent to which they utilize available security features. The study employed a descriptive approach utilizing a structured questionnaire for data collection via convenience sampling, through a sample of 174 customers. Statistical tools including proportion study, ANOVA, regression, correlation, and chi-square were applied for comprehensive data analysis. Factors influencing customers' awareness and perception of digital banking security will be analysed, shedding light on the adequacy and efficacy of existing security measures in online banking. This research is crucial in understanding the current landscape of digital banking security awareness among customers. By identifying gaps in knowledge and usage of security measures, banks and financial institutions can tailor their strategies to enhance customer protection and trust in digital banking systems, ultimately fortifying the security infrastructure of the financial sector.

Keywords: *Customer awareness, Digital banking, Financial sector, Online banking, Security protocols, Security threats*

1. INTRODUCTION

Digital banking has cemented the path to additional gamut of banking by permitting the patrons to perform their regular banking events at their accessibility. The Digital banking transactions in emerging nations like India are rising quickly due to the diffusion of internet and cell phones. This transition from traditional banking to convenience banking not only offers unparalleled convenience to users but also presents a significant chance to transition near cash free or nil cash culture. Bolstering this shift, the Government of Bharath has spearheaded various initiatives under the umbrella of 'Digital India,' aiming to foster a digitally vested environment characterized by impersonal, electronic, and cash free transactions.

However, amidst this transformative journey, the digital banking sector faces a plethora of security concerns and challenges. As the banking system undergoes distinct phases of digital transformation, propelled by escalating rivalry amid state owned, private, and overseas institutions, the imperative towards ensure security becomes

paramount. The goal of making banking more affordable, efficient, and accessible to all citizens must be balanced with the imperative of safeguarding sensitive financial data and transactions.

This research aims to investigate the diverse range of security issues and obstacles faced by digital banking in India. Through an examination of the evolving landscape of cyber threats, the vulnerabilities specific to digital banking platforms, and the regulatory measures designed to counter these risks, this study seeks to offer insightful perspectives on enhancing the security and reliability of digital banking operations. Through performing so, this study intends near brand a meaningful involvement to the current dialogue environment the reinforcement of digital banking systems, fostering a secure and accessible financial environment for all stakeholders.

OBJECTIVE OF THE STUDY: Primary

Objective:

To evaluate the overall awareness level among customers regarding security threats and issues in digital banking.

Secondary Objectives:

1. To identify the specific digital banking security threats that customers are most aware of.
2. To assess customers' understanding of security protocols and best practices while using net banking services.
3. To determine the extent to which customers utilize security features available in net banking platforms.
4. To identify the factors influencing customers' awareness and perception of digital banking security.
5. To evaluate the adequacy and efficacy of existing security measures in online banking.

.

2. REVIEW OF LITERATURE

Aslam Sayeed, Sharaddha Singh, (2024): Describe in the study which examines the impact of security concerns on e-banking adoption, blending qualitative and quantitative methods to explore customer perceptions. Qualitative insights reveal diverse security apprehensions, while quantitative analysis highlights trust as a mediating factor. Addressing these concerns with robust security measures and transparent communication strategies can enhance e-banking adoption, driving the sector's digital evolution amidst technological advancements and changing consumer preferences.

Patcha Bhujanga Rao, (2024) – in their study thoroughly explores cyber security challenges in online banking, emphasizing the need to understand and mitigate risks posed by cyber threats. It addresses issues such as phishing, malware, identity theft, and data breaches, along with regulatory hurdles and mobile banking vulnerabilities. Through its analysis, the research purposes to offer visions and suggestions to strengthen safety and trust in digital banking within the digital financial landscape.

Jane Smith, Chen Liu, (2024): In this study examines the intricate regulatory environment leading digital banking, spanning facts defense, virtual safety, and monetary guidelines. It investigates how regulatory bodies enforce compliance to alleviate threats and safeguard customer benefits. Additionally, the study traces the impact of governing adherence on secure system strategy and execution, analysing risk management and encryption practices to bolster digital infrastructures against cyber threats. Challenges such as inter country dealings and efforts towards governing synchronization are discussed, alongside incipient styles in governing machinery (RegTech) and the use of progressive analytics to improve amenability observing.

Diptiben Ghelani, Surendra Kumar Redd (2022): In today's digital age, safeguarding data against cyber threats is crucial, especially in mobile environments like airplanes and ships. We aim to enhance data security measures by leveraging machine learning, biometric recognition, and hybrid approaches. One proposed solution involves integrating

biometric impressions and digital signatures into banking systems, reducing intrusion risks and ensuring secure transactions.

Suganya K, (2022): The study discusses the perpetual threat cybercrime poses to the security of financial and business sectors, particularly in online banking. It emphasizes the need to raise awareness among customers about cyber threats and suggests staying updated on security measures to mitigate risks during digital transactions. The research underscores the importance of safeguarding sensitive financial data and advocating for proactive measures to combat cyber threats in online banking.

Haitham M. Alzoubi, Taher M. Ghazal (2022): Digital banking encounters security risks from hackers and fraudsters, necessitating robust measures like multiple verifications and data encryption. Existing research underscores cyber security threats as a major concern in digital banking, often underestimated by users. This study supports hypotheses from previous works through theoretical analysis, stressing the need for further research to enhance security measures.

Pavithra B, (2021): The study underscores the importance of digital banking for modern customers, highlighting its convenience and effectiveness. It defines digital banking as conducting financial transactions digitally without visiting a bank branch, thanks to technological advancements. The research work surveys 150 users to identify factors influencing customer perception and satisfaction, revealing a preference for smartphone-based digital banking due to convenience and instant fund transfers.

Abdul Qarib Stanikzai, Munam Ali Shah (2021): The financial sector, encompassing banks, insurance, and real estate firms, faces increasing cyber threats, exposing institutions to risks of extortion, fraud, and political interference. With over 1.2 billion adults globally having bank accounts, cybercriminals exploit vulnerabilities for profit. This research targets to evaluate present cyber safety measures' efficacy in combating financial crime and achieving business confidentiality, integrity, and availability (CIA), proposing recommendations for enhanced security protocols.

Sankararaman, G; Suresh, S; Kumar, M Naveen (2021)

Further procedural progressions in trade and imbursement schemes quizzed the flat of cyber safety in the consumers' structure. Cyber safety entices dominant implication due to weighty dependence in the current electronically emerging modern commercial biosphere. The research absorbed on the gathering of customers' sentiments to cyber safety. Records composed to view on cyber safety from 112 customers over convenience sample method. Occurrence examination and correlation have smeared to analyse the records.

Vishnuvaradhan B, B. Manjula, R. Lakshman Naik (2020) -The study delves into M-Banking, highlighting its growth due to improved Internet speed and device capabilities. It discusses its subsets alongside E-Banking, focusing on Indian banks' structures and digital banking types. Through surveys, it identifies five M-Banking service categories, analyzing functionalities, advantages, disadvantages, and security concerns.

Luigi Wewege, Jeo Lee, Michael C. Thomsett,: (2020): Fintech and telecom firms are reshaping banking with user-centric digital services, yet facing trust and regulatory challenges. Despite lacking scale, they're valued partners for incumbent banks in digital transformations. The shift to digital banking underscores the importance of infrastructure capabilities, API standardization, and adherence to regulatory frameworks like data protection laws and open banking directives.

Rashidah, Burhan, Roohie Naaz Farhat (2020): Internet banking, a vital service offered by financial institutions, faces increasing threats, particularly during the user login process. Current security measures, including one- time

passwords (OTPs), often lack usability and scalability. This paper reviews security mechanisms in e-banking, discussing the pros and cons of OTPs and other solutions while highlighting remaining challenges.

3. RESEARCH METHODOLOGY

In this study the researchers have implemented descriptive research design. New and printed records were utilised in the research study. The sample method adopted remained non probabilistic convenience sampling. As per standard table for sample size determination, sample size was determined as 384 based on the population size and level of significance .Out of 384 questionnaires sent through Google form only 212 were respondent and out of 212 only 174 was usable, hence the study comprises of data collected from 174 members from the research area and duly analyzed. A self-administered survey tool was utilised to gather facts from the respondents of the general public. Percentile analysis and Chi – Square tests ANOVA and Correlation tests were carried out in the research to analyse the collected data. The study was concentrated on Chennai City only.

4. Results and Discussion

Table 1: Demographic Profile of the Respondents

Variables	Options	Percentage of the Frequency%
Gender of the Respondents	1.Male	51.1
	2. Female	48.9
Education of the Respondents	1. School Education	10.3
	2. Diploma	2.9
	3. UG	59.8
	4. PG	21.3
	5. PhD	5.7
Age of the Respondents	1.Below 25	46.6
	2.25-40	36.2

	3.40-60	13.8
	4.Above 60	3.4
Monthly income of the respondents	Less than 25,000	37.9
	25,000 - 50,000	44.8
	50,000 - 75,000	16.1
	75,000 - 1,00,000	1.1
Family Size of the respondents	1. Two	9.5
	2. Three	26.7
	3. Four	36.2
	4. Five & Above	27.5
Occupation	Student	16.1
	Unemployed	4.0
	Employed	67.8
	Self Employed	7.5
	Retired	4.6

Source: Data collected through questionnaire

It is observed from Table 1 that out of 378 customers, the most of them (51.1%) were male. 46.6 % of respondents remained in the age group of below 25 years. It might be noticed that the most of the customers' (59.8%) educational level was UG. 44.8 % of the respondents' monthly earnings was concerning Rs.25000 to Rs.50000. In terms of family size of the respondents, the majority of the size is four (36.2%). Many of the respondents (67.8) are employed

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 4 (2024)
http://eelet.org.uk

Table 2: Digital Banking Insights

VARIABLE	OPTION	PERCENTAGE OF FREQUENCY
DURATION OF USAGE OF DIGITAL BANKING	Less than 1 Year	8.6
	1 Year - 2 Years	18.4
	2 Years - 5 Years	39.1
	More than 5 Years	24.7
	I don't use digital banking services	9.2
FREQUENCY OF USAGE OF DIGITAL BANKING SERVICES	Daily	62.1
	Weekly	12.1
	Monthly	1.7
	Rarely	16.7
	Never	7.5
PREFERRED CHANNELS FOR BANKING TRANSACTIONS (Multiple Response)	Online banking via website	21.30
	Mobile banking app	32.20
	ATM Services	60.90
	Digital payment apps	86.80
	Visit bank branch	20.10
FEEL THAT ONLINE BANKING IS SECURE AND THE PERSONAL INFORMATION IS WELL-PROTECTED	Strongly Disagree	2.9
	Disagree	12.6
	Neutral	17.2
	Agree	67.2

HAVE EXPERIENCED OR KNOW SOMEONE WHO HAS EXPERIENCED A CYBER ATTACK RELATED TO ONLINE BANKING	Strongly Disagree	2.9
	Disagree	61.5
	Neutral	7.5
	Agree	24.1
	Strongly Agree	4.0
THE TYPE OF SECURITY ISSUE THAT THE RESPONDENTS ARE MOST AWARE OF	Phishing scams	68.4
	Malware or virus attacks	19.0
	Identity theft	7.5
	Key loggers	2.9
	Skimming	2.3
KNOWLEDGE OF MANAGING CYBER ATTACKS	Contact the bank immediately	84.5
	File a report with the law enforcement	4.6
	Change password/PINs for affected accounts	9.8
	Place a fraud alert on credit reports	1.1

From the table it is experiential that 39.1% of the respondents are using online banking for 2-5 Years. It indicates that a majority of respondents (62.10%) use digital banking services on a daily basis. Digital payment apps are the most favored, chosen by 86.80% of respondents. 67.20% of respondents agree that online banking is secure and their personal information is well-protected. A majority (61.50%) disagree that they or someone they know has experienced a cyber-attack. The majority (68.40%) are familiar with phishing scams. 84.50% of respondents indicate that they would contact the bank immediately if faced with a security threat in online banking, emphasizing the importance of swift communication with financial institutions.

Table 3: Insights on Cyber Threats

VARIABLE	OPTION	PERCENTAGE OF FREQUENCY
Limiting online banking due to cyber threats	Strongly Disagree	4.0
	Disagree	37.9
	Neutral	14.9
	Agree	37.9
	Strongly Agree	5.2
LEVEL OF AWARENESS ON CYBERSECURITY MEASURES IMPLEMENTED BY BANK FOR ONLINE TRANSACTIONS	Strongly Disagree	1.7
	Disagree	15.5
	Neutral	16.1
	Agree	66.7
RESPONDENTS REGULARLY CHANGE PASSWORD/PINs FOR SECURITY PURPOSE	Strongly Disagree	1.1
	Disagree	28.7
	Neutral	6.3
	Agree	55.2
	Strongly Agree	8.6
LEVEL OF AWARENESS ON SECURITY RISK IN USING PUBLIC Wi-Fi NETWORKS FOR DIGITAL BANKING	Strongly Disagree	.6
	Disagree	7.5
	Neutral	5.7
	Agree	58.6
	Strongly Agree	27.6

LEVEL OF AWARENESS ON INSTALLING ANTI-VIRUS SOFTWARE FOR ONLINE BANKING SECURITY	Strongly Disagree	1.7
	Disagree	12.1
	Neutral	8.0
	Agree	62.1
	Strongly Agree	16.1
BELIEF IN ADOPTING MULTI- FACTOR AUTHENTICATION IS A BEST PRACTICE FOR ONLINE BANKING SECURITY	Strongly Disagree	1.1
	Disagree	4.0
	Neutral	5.7
	Agree	67.8
	Strongly Agree	21.3
LEVEL OF AWARENESS ON SHARING PERSONAL OR FINANCIAL INFORMATION ON UNSECURED PLATFORMS CAN LEAD TO IDENTITY THEFT	Strongly Disagree	1.1
	Disagree	4.0
	Neutral	5.7
	Agree	67.8
	Strongly Agree	21.3

A significant portion (37.90%) both agree and disagree that cyber threats have caused them to limit or reduce their online banking activities, reflecting a divided perspective on the matter. The majority of respondents (66.70%) agree that they are aware of the cyber security measures implemented by banks for online transactions. A majority (55.20%) agree that they regularly change their passwords/PINs, indicating a proactive approach to enhancing security. A significant majority of respondents (86.20%) either agree or strongly agree that there are security risks associated with using public Wi-Fi networks for digital banking. The majority of respondents (78.20%) either agrees or strongly agrees on the importance of installing antivirus software for online banking security. Specifically, 62.10% agree and 16.10% strongly agree, indicating a widespread recognition of the necessity of this cyber security measure. A majority of respondents (79.30%) either agree or strongly agree that adopting multi-factor authentication is a best practice for online banking security. A substantial majority of respondents (89.10%) either agree or strongly agree that sharing personal or financial information on unsecured platforms can lead to identity theft.

Table 4: Insights on Sharing Information

VARIABLE	OPTION	PERCENTAGE OF FREQUENCY
LEVEL OF AWARENESS ON RISK ASSOCIATED WITH PROVIDING THIRD PARTY FINANCIAL APPS OR SERVICES ACCESS TO ONLINE BANKING DATA	Strongly Disagree	1.1
	Disagree	9.8
	Neutral	10.9
	Agree	69.5
	Strongly Agree	8.6
CONSIDER ACCOUNT FEATURES WHEN CHOOSING AN ONLINE BANKING SERVICE	Strong password requirements	35.10
	Regular account monitoring alerts	54.60
	Fraud protection services	77.60
	24/7 customer support	78.20
	Biometric login options	58.60
OVERALL LEVEL OF SATISFACTION ON CUSTOMER SUPPORT PROVIDED BY BANK FOR ADDRESSING SECURITY CONCERNS AND INQUIRIES	Very dissatisfied	1.1
	Dissatisfied	7.5
	Neutral	28.2
	Satisfied	62.1
	Very satisfied	1.1
READING THE TERMS	Very Dissatisfied	1.1

AND CONDITIONS OR PRIVACY POLICIES OF THIRD PARTY FINANCIAL APPS BEFORE CONNECTING THEM TO ONLINE BANKING ACCOUNTS	Dissatisfied	4.6
	Neither agree or disagree	10.3
	Satisfied	82.8
	Very Satisfied	1.1
MEASURES THAT ENHANCES SECURITY OF DIGITAL BANKING TRANSACTIONS	Updating passwords/PINs	55.20
	Using two-factor authentication	58
	Avoiding public Wi-Fi networks for banking transactions	83.30
	Installing antivirus or security software regularly on devices	50.60
	Monitoring account activity regularly	28.70
TRUSTWORTHINESS IN DIGITAL BANKING SERVICES	Strongly Disagree	.6
	Disagree	14.9
	Neutral	24.1
	Agree	59.8
	Strongly Agree	.6

Awareness regarding the risks associated with providing third-party financial apps or services access to online banking data. A significant majority (78.10%) either agrees or strongly agrees with the notion that such actions carry risks. The risks associated with providing third-party financial apps or services access to online banking data. A notable majority (78.10%) either agrees or strongly agrees that such actions pose risks. The majority of respondents (63.20%) express satisfaction with the customer support provided by banks for addressing security concerns and inquiries. 83.30% advocate for avoiding public Wi-Fi networks for banking transactions, highlighting awareness of associated risks. The

majority of respondents (60.40%) either agrees or strongly agrees regarding their trustworthiness in digital banking services.

Table 5 - ONE WAY ANOVA

Null Hypothesis (H0): There is no significant relationship between the age of the respondents and frequency of usage of digital banking services.

Alternate Hypothesis (H1): There is a significant relationship between the age of the respondents and frequency of usage of digital banking services.

OUTPUT:

ANOVA					
How frequently do you use digital banking services?					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	95.537	3	31.846	21.821	.000
Within Groups	248.095	170	1.459		
Total	343.632	173			

RESULT:

Observed p-value is .000, which is less than conventional significance level.

H0 is rejected

H1 is accepted

Hence, there is a significant relationship between the age of the respondents and frequency of usage of digital banking services.

Table 6 -CORRELATION ANALYSIS

Null hypothesis (H0): There is no correlation between the duration of usage of digital transactions and the perception of online banking security.

Alternate hypothesis (H1): There is a correlation between the duration of usage of digital transactions and the perception of online banking security.

OUTPUT

Correlations			
		How long have you been using digital banking services?	I feel that online banking is secure and my personal information is well- protected.
How long have you been using digital banking services?	Pearson Correlation	1	-.166*
	Sig. (2-tailed)		.028
	N	174	174
I feel that online banking is secure and my personal information is well-protected.	Pearson Correlation	-.166*	1
	Sig. (2-tailed)	.028	
	N	174	174
*. Correlation is significant at the 0.05 level (2-tailed).			

RESULT

From the above table, the correlation between the duration of usage of digital banking and the perception of online banking security is 0.028. H0 is rejected and H1 is accepted

Hence, there is a significant relationship between the duration of usage of digital transactions and perception on online banking security.

Table 7 - CHI-SQUARE ANALYSIS

Null Hypothesis (H0):

There is no association between the Level of Education and level of awareness of cyber security measures.

Alternate Hypothesis (H1):

There is an association between the Level of Education and level of awareness of cyber security measures.

OUTPUT:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	197.314[a]	48	.000
Likelihood Ratio	144.473	48	.000
N of Valid Cases	174		

RESULT:

Observed p-value is .000, which is less than conventional significance level.

H0 is rejected

H1 is accepted

Therefore, there is an association between the Level of Education and level of awareness of cyber security measures.

Table 8 - CHI-SQUARE ANALYSIS

Null Hypothesis (H0):

There is no significant relationship between awareness of the potential risks associated with providing third-party financial apps or services access to online banking data and the age of the respondents.

Alternate Hypothesis (H1):

There is a significant relationship between awareness of the potential risks associated with providing third-party financial apps or services access to online banking data and the age of the respondents.

OUTPUT:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	82.413[a]	12	.000
Likelihood Ratio	71.817	12	.000
Linear-by-Linear Association	38.578	1	.000
N of Valid Cases	174		

RESULT:
Observed p-value is .000, which is less than conventional significance level.
H0 is rejected and H1 is accepted

Hence, there is a significant relationship between awareness of the potential risks associated with providing third-party financial apps or services access to online banking data and the age of the respondents.

5.2 SUGGESTIONS: To Bank:

- Develop targeted educational campaigns to raise awareness about security threats among different age groups, emphasizing the significance of regularly updating passwords and avoiding common pitfalls like reusing passwords.
- Explore the use of blockchain technology for secure and transparent transactions, leveraging its decentralized and immutable nature to prevent tampering and fraud.
- Encourage banks to enforce multi-factor authentication as a standard security measure for online transactions, thereby enhancing customer protection against unauthorized access.
- To bolster customer support channels, prioritize investment in specialized 24/7 services focused on addressing security concerns, providing guidance, and offering assistance to customers encountering potential security threats.
- Partner with cyber security professionals or firms to conduct regular security audits and assessments, ensuring that digital banking systems remain resilient against emerging threats.

To Customers:

- Frequently verify the mail correspondence and SMS for alarms from the financial facility supplier. Echo any illegal transaction witnessed to the bank/NBFC/Facility supplier instantaneously for blocking the card/account/ wallet, so as to avoid any added harms.
- Protect the cards and set everyday bounds for dealings. It may also set bounds and activate/deactivate for local/global use. This can edge damage due to scam.
- Cyber fraud can be avoided by being cautious while scanning a QR code for online transactions, never clicking on a link or file received through messages/emails from unknown sources.
- Do not be misinformed by advices suggesting credit of money on your behalf with RBI for overseas payments, unloading of command, or victories of the draw.
- Do not reveal the personal credentials to your bank/e-wallet account. Do not have common credentials for e-commerce/ social media sites and your bank account/email linked to a bank account. Evade banking through community, open or free systems.

5.3 CONCLUSION:

In conclusion this study underscores the critical importance of enhancing customer awareness regarding security issues and threats in digital banking. With the rapid evolution of fintech and digital banking services, it is imperative for customers to remain vigilant and informed about the threats related with electronic transactions. The study reveals that while a significant proportion of customers are aware of cyber security measures and best practices, there are still areas for improvement, particularly among certain demographic groups. Efforts to educate customers should be tailored to address specific age groups, educational backgrounds, and levels of digital literacy.

Furthermore, the study highlights the need for continuous collaboration between banks, regulatory bodies, and cyber security experts to strengthen security measures and mitigate emerging threats. Multi-factor authentication, robust customer support services, and proactive password hygiene practices are essential components of a comprehensive security framework. By fostering a culture of transparency, promoting access to educational resources, and prioritizing customer-centric security solutions, banks can instill greater trust and confidence in digital banking platforms. Ultimately, ongoing research and proactive initiatives are vital to ensuring that customers are empowered to navigate the digital banking landscape securely and confidently.

REFERENCES:

1. Chandra Sekhar, Manoj Kumar, An overview of cyber security in digital banking sector (January 2023), East Asian Journal of Multidisciplinary Research 2(1):43-52
2. Haitham M, Mohammad Kamrul Hasan, Cyber security threats on digital banking (May 2022), International conference on AI in cybersecurity
3. Haitham M. Alzoubi, Taher M. Ghazal, Cyber Security Threats on Digital Banking (2022), Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)
4. Patcha Bhujanga Rao, A STUDY ON CYBER SECURITY ISSUES AFFECTING ONLINE BANKING AND TRANSACTIONS**,** March 2024, International Journal of Advance Research And Innovative Ideas In Education 9(6)
5. Pavithra C. B, Factors affecting customers' perception towards Digital Banking Services, 2021, Turkish Journal of Computer and Mathematics Education (TURCOMAT), Volume 12, Issue 11 Pages 1608-1614.
6. Sachin Borgave, Parag Kalkar, A Review of Cyber Security Issues in Online Banking and Online Transactions (November 2022), International conference on AI in cybersecurity 20(18): 405-418
7. Sankararaman, G., S. Suresh, and M. Naveen Kumar. "A STUDY ON USERS OPINION ON CYBER SECURITY." *International Journal on Global Business Management & Research* 10.2 (2021): 61-68.
8. Shraddha Singh, Dr. Aslam Sayeed, The impact of security concerns on customers' adoption of e-banking services (2024), International Research Journal of Modernization in Engineering Technology and Science, Volume 6, Issue 2.
9. Tan Kian Hua, Surendra Kumar Reddy, Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking (2022), American Journal of Computer Science and Technology, Volume 12, Issue 5.
10. Vishnuvardhan B, B Manjula, R Lakshman Naik (2020), A study of digital banking: Security issues and challenges, Third International Conference on Computational Intelligence and Informatics,Volume X, Issue 1, Page No 163-185
11. Yogesh Borse, Security challenges to Indian banking and financial sectors (September 2023), Juni Khyat Journal 13(2).