RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 07, Issue 03 March

Check for updates

http://dx.doi.org/10.47392/IRJASH.2025.020

Securing Fintech: Evaluating the impact of multi–factor authentication on Cyber Threats

Shivani Kumari[1], Kundana Sindhu[2], Dr.K. Krishna Kumari[3]

[1,2] PGDM Student, Indus Business Academy, Bangalore, Karnataka, India.

[3]Assistant Professor, Indus Business Academy, Bangalore, Karnataka, India.

Email ID: *shivanigupta3159@gmail.com[1], kundenasindhu8@gmail.com[2], krishna.k@iba.ac.in[3]*

Article history

Received: 05 February 2025
Accepted: 13 February 2025
Published: 21 March 2025

Keywords:
FinTech, MFA, cyber risks, fintech platforms, cybersecurity.

Abstract

FinTech's rapid expansion has transformed financial services but also heightened cyber threats, demanding stronger security measures. Multi-Factor Authentication (MFA) enhances protection by requiring multiple verification factors, reducing unauthorized access and financial fraud.
This study examines the relationship between demographic factors (age, gender, occupation, income) and users' perceptions of security in FinTech platforms with MFA. It also assesses MFA's impact on users' confidence in FinTech security. Using a sample of 100 respondents, ANOVA and descriptive statistics analyze both qualitative and quantitative data, offering insights for policymakers and cybersecurity stakeholders.

1. Introduction

The integration of Multi-Factor Authentication (MFA) significantly enhances security in financial transactions compared to static passwords, which remain vulnerable to phishing, credential stuffing, and other cyber threats. MFA employs multiple authentication factors knowledge (passwords or PINs), possession (tokens or mobile devices), and inherence (biometric indicators like fingerprints or facial recognition) to create a robust defense against unauthorized access. Despite its advantages, cyber threats continue to evolve, impacting transaction security. Prior research highlights MFA's role in mitigating cyber risks on fintech platforms. Meyer et al. (2023) found that accounts with MFA on Microsoft Azure Active Directory had a compromise rate of less than 0.01%, reinforcing its effectiveness. However, Wee et al. (2024) identified vulnerabilities in existing MFA protocols, emphasizing the need for continuous improvements. Nair and Song (2023) proposed advanced hashing techniques to strengthen MFA security while maintaining usability. Kandula et al. (2023) explored MFA's role in Zero Trust Architecture, advocating adaptive authentication, while Guma (2023) examined the balance between security and usability. Building on these findings, this study evaluates MFA's impact on fintech security, particularly in financial transactions. It also examines how demographic factors (age, gender, occupation, income) influence users' perceptions of security and confidence in fintech platforms.

2. Literature Review

As fintech adoption grows, so do cyber threats, making MFA a critical security measure. Meyer et al. (2023) demonstrated that MFA significantly reduces unauthorized access, with application-based methods proving more secure than SMS-based authentication. Similarly, Wee et al. (2024) identified security gaps in MFA protocols, suggesting enhancements to counter evolving threats. Nair and Song (2023) introduced a multi-factor credential hashing function, improving security against brute-force attacks while

preserving usability. Kandula et al. (2023) examined MFA's integration into Zero Trust Architecture, emphasizing adaptive authentication based on contextual factors. Guma (2023) explored the trade-off between security and usability, proposing solutions that maintain high protection levels without compromising user experience. These studies reinforce MFA's role in enhancing fintech security while highlighting areas for refinement. This research expands on these insights by assessing MFA's effectiveness in securing financial transactions and improving user confidence in fintech platforms. [1-3]

3. Research Methodology

This study employs both qualitative and quantitative methods to evaluate the impact of Multi-Factor Authentication (MFA) on FinTech security. A random sampling approach is used to gather insights from 100 respondents, including students, professionals, and entrepreneurs. The research aims to:

3.1. Research Objectives

- To explore the relationship between demographics factors (age, gender, occupation, income) and users' perceptions of security and confidence in Fintech platforms with Multi-Factor Authentication.
- To examine the impact of Multi-Factor Authentication (MFA) on users' perceptions of security and their confidence in FinTech platforms.

3.2. Data Collection

3.2.1. Primary Data

Primary data is collected through a structured questionnaire targeting frequent FinTech users. Respondents share their experiences, concerns, and perceptions regarding MFA's effectiveness in preventing cyber threats.

3.2.2. Secondary Data

Existing research, cybersecurity reports, and FinTech security studies provide secondary data. A literature review identifies key findings, research gaps, and emerging threats, supporting a deeper understanding of MFA's role in FinTech security.

3.3. Sampling Size & Demographics

A sample of 100 respondents from diverse backgrounds ensures a broad analysis of how age, occupation, and income influence cybersecurity perceptions and digital trust in FinTech services.

4. Data Analysis

The analysis of the statistical data obtained from a sample of 100 respondents shows important trends about the role of MFA in respect of protection from cyber threats. Visualizing insights through Tableau enhances clarity, making it easier to interpret user experiences and security perceptions. This approach provides reliable conclusions on FinTech security and MFA's effectiveness.

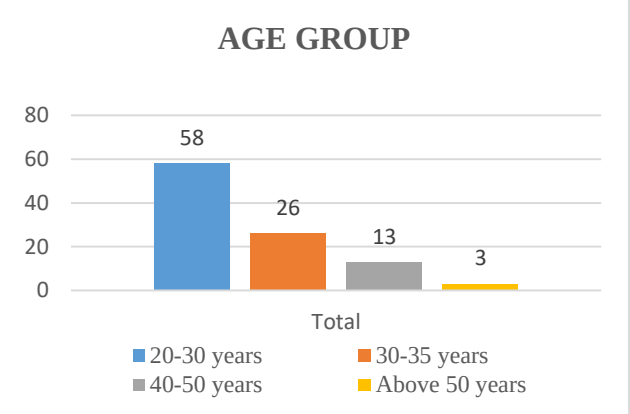

Figure 1 Age Group Graph

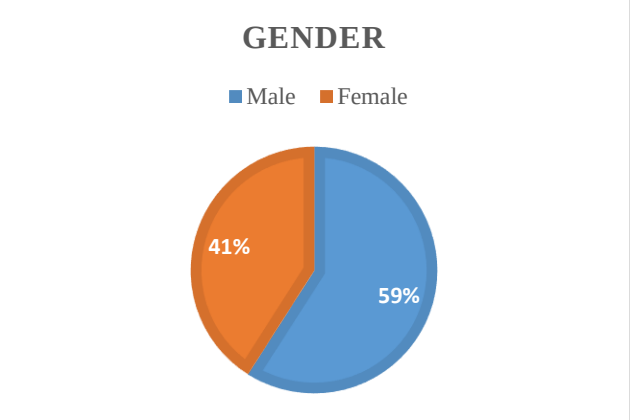

Figure 2 Gender Graph

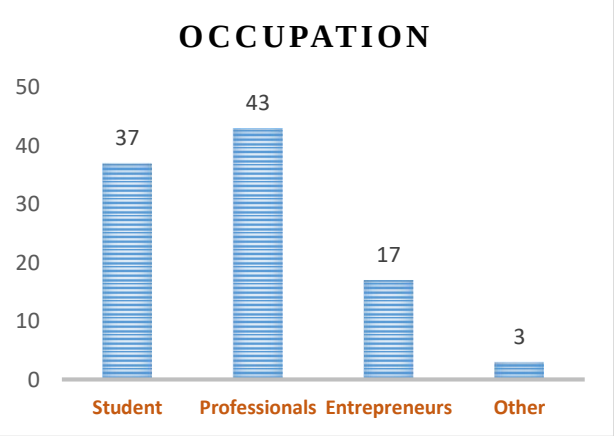

Figure 3 Occupation Graph

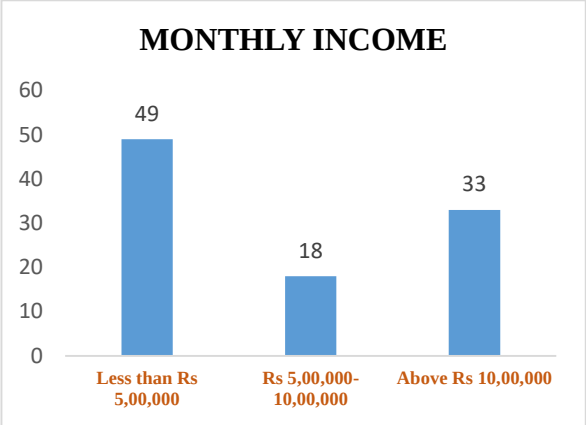

Figure 4 Monthly Income Graph

4.1. Interpretation

The demographic information provides a perspective, with the maximum proportion of 58% respondents falling within the age bracket of 20-30 years, then followed by 26% between the ages of 30-35. This shows that a significant proportion of younger audience is involved. The male-to-female ratio showed a distribution of 59% and 41% respectively, with fairly balanced representation. In the job division, the professionals occupy the major proportion (43%), followed by students at 37% and entrepreneurs at a slightly lower percentage, standing at 17%. The income distribution suggests that 49% earns below Rs. 500000, while 33% earn over Rs. 10,00,000, indicating the need for diversity in financial backgrounds. This wide-ranging sample ensures a fair assessment of the influence of MFA on the perception of cybersecurity across diverse sexes or generational cohorts. Table 1 shows Descriptive Statistics

Table 1 Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q1. Age	100	1	4	1.61	.827
Q2.Gender	100	1	2	1.41	.494
Q3.Occupation	100	1	4	1.86	.804
Q4.Income	100	1	3	1.84	.896
Q5.How long have you been using FinTech services?	100	1	4	2.36	1.069
Q6.Have you ever experienced a cyber-threat while using a fintech platform?	100	1	2	1.33	.473
Q7.If 1, please specify the type(s) of cyber threat you encountered mostly	100	1	5	3.14	1.551
Q8.How did the cyber threat impact you?	100	1	4	2.28	1.055
Q9.What security measures do you think fintech platforms should prioritize to prevent cyber threats?	100	1	5	2.59	1.393
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [1.1(MFA) enhances my sense of security when using FinTech platforms]	100	2	5	4.11	.952
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [2. 1 makes me more cautious about the security of my financial	100	2	5	4.01	.959

transactions.]					
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [3. 1 encourages me to use FinTech services more frequently]	100	2	5	4.01	.990
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [4. I believe 1 is effective in preventing 3 to my accounts.]	100	2	5	3.97	1.020
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [5. I am willing to go through 1 even if it takes extra time to access services.]	100	2	5	4.11	.920
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [6. 1 has made me more aware of potential cybersecurity threats in FinTech through regular security update and awareness programs.]	100	2	5	4.06	.952
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [7. I feel safer and confident conducting financial transactions online due to the presence of 1.]	1+300	2	5	4.00	.985
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [8. I am more likely to trust FinTech companies that utilize 1.]	100	2	5	4.09	.986
Q11.How 3 do you face problems accessing your accounts due to MFA?	100	1	3	1.65	.783
Q12.On a scale from 1 to 5, how satisfied are you with the overall cybersecurity measures of the fintech platforms you use?	100	2	5	4.04	.974
Valid N (list wise)	100				

4.2. Interpretation

The descriptive statistics that the majority of respondents are younger, with a mean age score of 1.61 and low variability, indicating a consistent perception of security across age groups. The gender distribution, with a mean score of 1.41, shows a predominance of one gender, hinting at a potential gender-related trend in perceptions of security, through further analysis is needed. Occupation variability (mean1.86, SD 0.0804) implies that individuals in different professionals may have different views on the role of MFA in enhancing security. With a mean income score of 1.84 and moderate variability, it appears that users from lower income brackets dominate the sample, suggesting that income could influence the level of trust or confidence in MFA, as those with higher incomes might prioritize security more due to perceived risks. [4-5]

4.2.1. Hypothesis Testing

- Null Hypothesis (H_0): MFA does not significantly impact users' perception of security or confidence in FinTech platforms.
- Alternative Hypothesis (H_1): MFA significantly impacts users' perception of security and confidence in FinTech platforms.

Table 2 Anova

		Sum of Squares	df	Mean Square	F	Sig.
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [1. 1(MFA) enhances my sense of security when using FinTech platforms]	Between Groups	70.368	3	23.456	115.940	<.001
	Within Groups	19.422	96	.202		
	Total	89.790	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [2. 1 makes me more cautious about the security of my financial transactions.]	Between Groups	67.391	3	22.464	91.379	<.001
	Within Groups	23.599	96	.246		
	Total	90.990	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [3. 1 encourages me to use FinTech services more frequently]	Between Groups	65.584	3	21.861	66.825	<.001
	Within Groups	31.406	96	.327		
	Total	96.990	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [4. I believe 1 is effective in preventing 3 to my accounts.]	Between Groups	74.266	3	24.755	82.968	<.001
	Within Groups	28.644	96	.298		
	Total	102.910	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [5. I am willing to go through 1	Between Groups	58.991	3	19.664	76.120	<.001
	Within Groups	24.799	96	.258		

even if it takes extra time to access services.]	Total	83.790	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [6. 1 has made me more aware of potential cybersecurity threats in FinTech through regular security update and awareness programs.]	Between Groups	67.913	3	22.638	100.025	<.001
	Within Groups	21.727	96	.226		
	Total	89.640	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [7. I feel safer and confident conducting financial transactions online due to the presence of 1.]	Between Groups	75.648	3	25.216	118.943	<.001
	Within Groups	20.352	96	.212		
	Total	96.000	99			
Q10.Please rank the statement given below according to your opinion on MFA reducing risk [8. I am more likely to trust FinTech companies that utilize 1.]	Between Groups	83.803	3	27.934	216.494	<.001
	Within Groups	12.387	96	.129		
	Total	96.190	99			

4.3. Interpretation

The ANOVA results indicate that Multi-Factor Authentication (MFA) significantly impacts users' perceptions of security and confidence in FinTech platforms. The p-values (<.001) across all statements confirm that differences in user opinions are statistically significant. Higher F-values suggest a strong effect of MFA on security awareness, trust, and willingness to use FinTech services. Users feel safer, more cautious about security risks, and more likely to engage with FinTech platforms implementing MFA. These findings support the alternative hypothesis (H_1) that MFA enhances security perceptions and confidence in FinTech services. [6-8]

5. Findings

- The study finds that younger respondents dominate the sample, with a consistent perception of security across age groups.
- Gender distribution suggests a potential trend in security perceptions, but further analysis is needed to confirm its significance.
- Different occupations exhibit varied opinions on MFA's role in security, indicating that professional background may influence security concerns.
- Income levels appear to impact trust in MFA, with lower-income users dominating the sample. Higher-income users may have heightened security awareness due to greater perceived financial risks.
- ANOVA results confirm that MFA significantly influences users' security perceptions, trust, and willingness to engage with FinTech platforms.
- The p-values (<.001) indicate that differences in user opinions are statistically significant, supporting the alternative hypothesis (H_1).
- Higher F-values suggest that MFA has a

strong effect on security awareness, trust, and users' willingness to use FinTech services.

- Users feel safer, more cautious about security risks, and more likely to engage with FinTech platforms that implement MFA.
- MFA plays a crucial role in increasing users' confidence in online financial transactions, enhancing digital trust in FinTech platforms.
- FinTech companies should enhance MFA awareness among diverse demographic groups to ensure inclusivity in cybersecurity practices.
- Tailoring security education programs for different professional backgrounds may help improve trust and adoption of MFA.
- Companies should explore user-friendly MFA solutions to maintain security while ensuring a seamless experience.
- Targeted security campaigns could encourage higher-income users to recognize the benefits of MFA beyond financial protection.
- Future research should explore gender-related trends in cybersecurity perceptions for better-targeted security strategies.
- FinTech platforms should continue strengthening MFA while balancing security with usability to improve customer satisfaction.
- Regular security awareness programs can further enhance users' cautiousness and trust in digital financial services.
- MFA plays a critical role in enhancing security perceptions and trust in FinTech services.
- Users across age, occupation, and income groups show varying attitudes toward MFA, highlighting the need for tailored security measures.
- The findings emphasize the necessity of ongoing improvements to MFA to keep pace with evolving cyber threats.
- While MFA is effective in preventing security risks, companies must balance security with usability to encourage broader adoption.
- Strengthening MFA awareness and refining its implementation can significantly enhance user confidence in FinTech platforms.
- The statistically significant ANOVA results confirm that MFA positively influences users' trust, security awareness, and willingness to engage with FinTech services.

6. Recommendation

To enhance security perceptions and trust in FinTech platforms, companies should focus on increasing MFA awareness across diverse user demographics. Tailored security education programs can address varying concerns based on occupation and income levels, ensuring inclusivity. Simplifying MFA processes while maintaining robust security measures can encourage broader adoption. Regular security awareness initiatives can further strengthen digital trust and cautious financial behaviour.

Conclusion

The study confirms that MFA significantly impacts users' confidence in FinTech platforms, with statistical evidence supporting its effectiveness in enhancing security awareness and trust. While MFA is a crucial cybersecurity tool, its usability must be balanced with security measures to ensure user convenience. Continuous improvements and targeted awareness campaigns will help optimize MFA adoption, making FinTech services both secure and user-friendly.

Reference

[1]. Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). How effective is multifactor authentication at deterring cyberattacks? arXiv preprint arXiv:2305.00945.

[2]. Wee, A. K., Chekole, E. G., & Zhou, J. (2024). Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis. arXiv preprint arXiv:2407.20459.

[3]. Nair, V., & Song, D. (2023, July). Multi-factor credential hashing for asymmetric brute-force attack resistance. In 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P) (pp. 56-72). IEEE.

[4]. Kandula, S. R., & Kassetty, N. (2024). Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication. International Journal of Global Innovations and Solutions (IJGIS).

[5]. Ali, G., Dida, M. A., & Elikana Sam, A. (2021). A secure and efficient multi-factor authentication algorithm for mobile money applications. Future Internet, 13(12), 299.

[6]. Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2023). Role of authentication factors in Fin-tech mobile transaction security. Journal of Big Data, 10(1), 138.

[7]. Idayani, R. W., Nadlifatin, R., Subriadi, A. P., & Gumasing, M. J. J. (2024). A comprehensive review on how cyber risk will affect the use of Fintech. Procedia Computer Science, 234, 1356-1363.

[8]. Guma, A. (2023). Balancing security and usability in fintech authentication systems. Journal of Cybersecurity Research, 12(3), 45-60.