Student's Perception Towards Biometric Authentication in FinTech Platforms

Anaswara Manoharan| Dr.Abdul Salam.K

Research Scholar P.G and Research Department of Commerce Government College Mananthavady, Affiliated to Kannur University

Associate Professor and Research Supervisor P.G and Research Department of Commerce Government College Mananthavady, Affiliated to Kannur University

Abstract: The rapid emergence of financial technology, or FinTech, has significantly altered how financial services are provided and accessed. In FinTech platforms, biometric authentication—which includes fingerprint scanning, facial recognition, and iris recognition—has become a popular security feature. Students' perceptions of biometric authentication in FinTech applications are investigated in this study, with an emphasis on usability, security, convenience, trust, and privacy concerns. A structured questionnaire was used to gather information from college students. The study examines students' perceptions of biometric authentication and various factors influencing their acceptance of these technologies in financial transactions. The results show that while most people view biometric authentication as a safe and practical way to access financial services, privacy and data protection issues persist. For the purpose of to increase user trust, the study emphasizes the significance of enhancing awareness, transparency, and data security practices in FinTech platforms. The findings give policymakers, financial institutions, and FinTech developers helpful information for creating more user-friendly and safe authentication systems.

Keywords: FinTech, biometric authentication, digital payments, security perception, privacy concern, student users.

INTRODUCTION

Financial technology, also known as FinTech, has emerged quickly as a result of the digital transformation of financial services. FinTech refers to the application of technology to financial services with the aim of improving the user experience, accessibility, and efficiency of financial services. Currently, many people are using digital wallets, online payment systems, and mobile banking services, especially young people and students.

However, today, many people are concerned about fraud and security, especially regarding the increased adoption of digital financial services. Conventional methods of security, such as PINs and passwords, are often at risk of identity theft, phishing, and hacking. In order to improve security and user experience, many financial institutions and technology companies are adopting biometric technologies.

Biometric authentication relies on the unique biological characteristics of an individual, such as fingerprints, facial recognition, voice recognition, or iris scanning, in order to verify identity. Biometric authentication is more secure than traditional methods of authentication because it is difficult to replicate these characteristics. Biometric authentication also provides faster access to financial services, and there is no need to remember complex passwords.

The group of users that is most actively using FinTech services is students. Students are an important group to study the adoption of biometric authentication because they actively use mobile devices and digital payment services. Financial institutions can develop secure and friendly systems by considering the perception of biometric authentication among students.

In order to ensure security in digital financial transactions, authentication plays a vital role. In traditional methods of authentication, like passwords and personal identification numbers (PINs), there are various limitations, including identity theft, phishing, and hacking. Biometric authentication systems have become more popular in FinTech services due to the limitations of traditional systems. In order to authenticate the identity of a user, biometric systems use specific biological features like voice recognition, iris scan, fingerprint scan, and face recognition.

Owing to the convenience and enhanced security that biometric authentication provides, it is being increasingly incorporated into digital wallets, mobile banking applications, and payment systems. Currently, many smartphones are equipped with biometric authentication functionality, enabling users to quickly and securely authenticate financial transactions. Despite the convenience and security that biometric authentication provides, users are still concerned about the security of their data, privacy, and potential misuse of biometric information.

Students, owing to their heavy usage of mobile applications and digital payment systems, form a substantial group of users of digital financial services. Student perceptions of biometric authentication may influence the future adoption and acceptance of these technologies. It is, therefore, essential for financial institutions and technology companies to understand the views of students regarding the security, convenience, and privacy aspects of biometric authentication.

The objective of this study is to identify the perceptions of students in relation to biometric authentication in FinTech, with special emphasis placed on key factors like utility, security, trust, and privacy.

LITERATURE REVIEW

(Mirza et al., 2018),The study looked into how Bahraini mobile banking users accept fingerprint authentication as a biometric security method. It examined the factors that affect user acceptance by using an extended Technology Acceptance Model (TAM). Data was collected from 315 bank customers, and SPSS was used for analysis. The results showed that users generally had a positive view of this biometric

technology. They also indicated that several factors significantly impacted users' willingness to adopt fingerprint authentication in mobile banking.

(Bermeo-Giraldo et al., 2023), The factors that affect the adoption of FinTech services were examined in a study conducted among Colombian university students. The data was collected from 124 university students using a quantitative approach. The findings indicated that low regulation had little impact, but social influence and financial education had a positive impact on the perceived benefits of FinTech services. The study also found that while the use of mobile is rapidly increasing, the adoption of FinTech is still quite slow, and many students are using FinTech services without understanding the concept.

(Kang, 2018), The research carried out on mobile FinTech payment services sought to understand the impact of information technology breakthroughs and the rise in the use of mobile devices, which have contributed to the rapid development of digital payment technology. The research considered the current developments in mobile FinTech payments, with service providers being categorized into different groups. Notably, financial institutions, hardware producers, operating systems, and payment platforms were considered. Additionally, the importance of data integrity, privacy, authorization, authentication, and availability was highlighted. Security was also emphasized as an essential requirement in the development of mobile FinTech payments.

(Khan et al., 2023), The role of authentication technologies in improving the security of mobile financial transactions was explored in a review study. The study identified different approaches to improving user authentication and reducing fraud in digital financial transactions by analyzing 92 research publications. The findings highlighted the importance of technologies such as QR codes and multi-factor authentication in improving the security of financial transactions. According to the findings of the study, advanced authentication methods can help in verifying the authenticity of users, detecting potential risks, and reducing the chances of fraudulent transactions of mobile money.

(Wang, 2021), Incorporating the concepts of perceived trust and perceived privacy into the Technology Acceptance Model, a study examined user acceptance of biometric identification in FinTech applications. The findings of the study revealed that user acceptance of biometric technology is significantly driven by privacy and trust concerns, and that the most widely used authentication method in FinTech services is voice and facial recognition.

(Al-Debei et al., 2024), In addition, the factors that influence the intention to adopt this technology were examined in a study about iris recognition technology for authentication in FinTech ATMs. The study revealed that, for instance, concerns about privacy, financial, and physical risks have a significant influence on the intention to adopt the technology, while advantages such as financial security, convenience, and hygiene have a positive influence. According to the study, the perceived value of the technology is an important factor in its adoption.

(Liébana-Cabanillas et al., 2026), The factors that affect the adoption of biometric payment cards in electronic transactions were examined in a study. The findings, which were derived from an online survey and structural equation modeling, indicated that social influence and perceived risk had little impact, but factors related to technology acceptance and trust had a significant effect on users' intention to use and recommend biometric payment cards. The study highlights the importance of building users' confidence in order to promote the adoption of biometric payment systems.

OBJECTIVES OF THE STUDY

- To examine students' awareness of biometric authentication in FinTech platforms
- To analyse their perception regarding security, convenience, and usability
- To identify privacy concerns associated with biometric authentication
- To study the relationship between trust and adoption of biometric systems

RESEARCH METHODOLOGY

Research Design

The present study used a descriptive research design in order to investigate and analyze the perception of students on biometric authentication in FinTech services. Patterns, attitudes, and opinions regarding certain variables, such as security, convenience, usability, trust, and privacy concerns, can be determined in the study.

Sources of Data

Both primary and secondary data are used for this purpose.

• Primary Data: The structured questionnaire was used as a tool for direct data collection for this study. The questionnaire was used for collecting the opinions of students on various aspects related to biometric authentication, such as reliability, usability, and data privacy concerns.

• Secondary Data: Various academic journals, books, reports, and the internet were used as secondary data sources for this study. These sources were used for gaining theoretical and conceptual insights into the concept of biometric authentication in financial technology.

Sampling Technique and Sample Size

A total of 120 college students were selected as the sample for the study. The sampling method used for selecting the respondents was convenience sampling, in which willingness and accessibility were taken into

consideration. Students familiar with digital payment systems and various biometric authentication techniques are represented in the sample.

Tools and Techniques for Analysis

In order to draw significant conclusions, the data collected was methodically analyzed using appropriate statistical tools.

Percentage analysis: This method was used to show the distribution of the results and draw general patterns in the views of the students.

Mean Score Analysis: This method uses a Likert scale to measure the average level of agreement or perception regarding various variables.

Correlation analysis: This method was used to determine the factors affecting the acceptance of biometric authentication by establishing the correlation between various significant variables such as security, trust, convenience, and privacy concerns.

RESULTS AND ANALYSIS

1 Percentage Analysis

Factor	Agree (%)	Neutral (%)	Disagree (%)
Biometric authentication is secure	72%	18%	10%
Easy to use	78%	12%	10%
Convenient for transactions	80%	10%	10%
Trustworthy system	65%	20%	15%
Concern about privacy	60%	15%	25%

Most students think biometric authentication is convenient and easy to use. Nonetheless, a sizable percentage (60%) voice privacy concerns, suggesting a lack of total faith in the system.

2 Mean Score Analysis

(Scale: 1 = Strongly Disagree, 5 = Strongly Agree)

Variable	Mean Score
Security	4.1
Convenience	4.3
Usability	4.2
Trust	3.8
Privacy Concern	3.6

Convenience has the highest mean score, showing strong agreement among respondents. Privacy concern has a moderate score, indicating that while students accept the technology, they remain cautious about data security.

3 Correlation Analysis

Variables	Correlation Coefficient (r)
Security & Trust	0.68
Convenience & Usage	0.72
Privacy Concern & Trust	-0.55

The findings indicate that students are more likely to trust a biometric authentication system if they think that it is more secure. The convenience of using the authentication system is another significant aspect that has to be taken into consideration, as users are more likely to use a system that is more convenient. On the other hand, privacy-related concerns seem to destroy trust, suggesting that a biometric authentication system is less trusted when users are more concerned with security.

DISCUSSION OF RESULTS

The results indicate that students generally have a positive perception of biometric authentication, especially due to the ease of use and convenience of the method, which is good news for the acceptance of FinTech services that incorporate this method of authentication. On the other hand, the issue of privacy and the possible misuse of their information remains a major concern, despite the security benefits of the method, as the students' trust is largely dependent on the level of protection of their information.

FINDINGS

- Students are highly aware of biometric authentication systems
- Convenience and ease of use are the main factors driving adoption
- Security is perceived positively but not without doubts
- Privacy concerns significantly affect trust levels
- Trust is strongly linked with perceived security

SUGGESTIONS

- FinTech companies should improve **data protection mechanisms**
- Awareness programs should be conducted to educate users about biometric security
- Clear privacy policies must be communicated to users
- Government regulations should ensure safe handling of biometric data

CONCLUSION

Nowadays, FinTech platforms incorporate biometric authentication as one of the key components of the technology, offering greater ease and security to the users. As per the study, students are found to be open to the technology as well. However, the major challenge faced by the technology in terms of total acceptance and trust remains the privacy factor. To promote the technology of biometric authentication in digital financial services in the future, the issues related to privacy need to be addressed with greater security measures.

REFERENCE

- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems*, 14(1), 4–20.
- Reserve Bank of India (RBI). (2022). *Digital Payment Security Guidelines*.
- Gupta, S., & Arora, N. (2021). Adoption of biometric authentication in digital payments. *Journal of Financial Technology*, 8(2), 45–60.
- Al-Debei, M. M., Hujran, O., & Al-Adwan, A. S. (2024). Net valence analysis of iris recognition technology-based FinTech. *Financial Innovation*, *10*(1), 59. https://doi.org/10.1186/s40854-023-00509-y

- Bermeo-Giraldo, M. C., Valencia-Arias, A., Palacios-Moya, L., & Valencia, J. (2023). Adoption of Fintech Services in Young Students: Empirical Approach from a Developing Country. *Economies*, *11*(9), 226. https://doi.org/10.3390/economies11090226
- Kang, J. (2018). Mobile payment in Fintech environment: Trends, security challenges, and services. *Human-Centric Computing and Information Sciences*, *8*(1), 32. https://doi.org/10.1186/s13673-018-0155-4
- 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. https://doi.org/10.1186/s40537-023-00807-3
- Liébana-Cabanillas, F., Irimia-Diéguez, A., Albort-Morant, G., & Zarco, C. (2026). Unlocking the future of paytech: Exploring biometric payment card adoption patterns. *Financial Innovation*, *12*(1), 84. https://doi.org/10.1186/s40854-025-00883-9
- Mirza, Z., Alsalem, E., Mohsin, F., & Elmedany, W. M. (2018). Users' Acceptance of Using Biometric Authentication System for Bahrain Mobile Banking. *KnE Engineering*, *3*(7), 102. https://doi.org/10.18502/keg.v3i7.3075
- Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, *7*(1), 42. https://doi.org/10.1186/s40854-021-00260-2