

A Study on Impact of Fintech on Cybersecurity Challenges on Digital Economy

Paramadevanapalli Thanuja¹, Bagali Ambreen²

¹Student of 4th semester (USN: 3BR24BA126) Department of Management Studies, Ballari Institute of Technology and Management, Ballari, Karnataka, India.

²Assistant Professor, Department of Management Studies, Ballari Institute of Technology and Management, Ballari, Karnataka, India.

Abstract—The financial technology (FinTech) has revolutionized the digital economy through providing quick, easy-to-access banking services. Nevertheless, there is an increase to cyber threats like phishing attacks; identity theft; hacking incidents on social media sites. The paper is about FinTech's effect on cyber security issues and Artificial Intelligence (AI), blockchain technology, biometrics for enhancing information safety. Data were collected from 250 FinTech users of Ballari district by means of a structured questionnaire. These results show that although there is a high level of adoption of fintech products and services there needs to be better security measures and awareness among consumers so that they can safely conduct their business online.

I. INTRODUCTION

FinTech has transformed finance through electronic means which simplify banking, payment services; loans and insurance and investments. AI, blockchain, cloud computing, big data analytics, and mobile applications help people to get access to banking services faster, easier and cheaper.. The digital economy relies upon widespread adoption of electronic technology & internet based services to conduct commercial activities, banking operations etc. Digitalization has an impact on banking today. Today people, companies and government use computer for banking because they are faster than manual work with this machine. However it increases your chances to get hacked by hackers on banks (and others). With an increase rate for online banking and payment systems, hackers are able to access these bank accounts by means of phishing attack, identity theft, ransomware attack, data breach, and fraud on

customers' money.

II. LITERATURE REVIEW

1. Faheem Ashraf and Sadi Badi (2025), their research Cyber Risk and Data Privacy in FinTech Strengthening Fraud Detection, Financial Institutions Security, and Regulatory Compliance, stated that FinTech has changed financial services by making them faster and more accessible. However, it has resulted from cybercrimes like frauds, identity thefts and data breaches due to fast technological progress. AI, blockchain technology; biometrics are some of them that help improve fraud detection; strengthen banking security and ensure regulatory compliance.

2. Malvika Souran (2025), Cybersecurity Challenges and Strategic Defenses in FinTech, A Review of Emerging Threats and Mitigation Frameworks studied the increasing cybersecurity threats faced by FinTech organizations, including phishing, malware, ransomware, and online scams. This research found out to be successful with ai, cryptography, blockchain technology and Zero Trust model for protecting important banking information.. and minimizing cyber risks.

3. Adetunji Paul Adejumo and Chinonso Peter Ogburie (2025), The Role of Cybersecurity in Safeguarding Finance in a Digital Era, discussed the critical role of cybersecurity in protecting financial institutions against increasing digital threats .The study found

that advanced security solutions including AI, blockchain, encryption, and multi-factor authentication play a vital role in securing financial transactions, safeguarding customer information, and maintaining trust in digital financial systems.

4. Muhammad Danish and Rohit Donni (2025), *Cybersecurity Challenges in Digital Services Managing Risk in a Rapidly Evolving FinTech Landscape*, stated that although FinTech has improved digital financial services, it has also created new cybersecurity challenges such as fraud and data breaches. They stressed on strong cyber security measures; risk management strategies and compliance with laws for protecting online banking systems.

5.

6. Ashish Juneja, Shankha Subhra Goswami, and Surajit Mondal (2024), in *Cyber Security and Digital Economy: Opportunities, Growth and Challenges*, stated that cybersecurity has become a basic requirement for. online retail, e-commerce and electronic payment systems are growing at an unprecedented nowadays. This research found out that strong cyber security measures should not only help to prevent cyber frauds but also minimize losses on account of customers' confidence.

7. Adeyemi Akinyemi (2024), *Cybersecurity in FinTech and Digital Payment Systems*, explained that the rapid expansion of FinTech and digital payment systems has increased cybersecurity threats such as phishing, malware, fraud, and data breaches. The study suggested that encryption, blockchain, artificial intelligence, and multi-factor authentication are effective tools for protecting financial data and ensuring secure transactions.

8. Paulin K. Kamuangu (2024), *A Review on Cybersecurity in FinTech: Threats, Solutions, and Future Trends*, observed that although FinTech has enhanced the accessibility and efficiency of financial services, it has also increased cybersecurity risks. The study recommended the adoption of AI, blockchain technology, and biometric authentication to strengthen security and protect customer information.

9. Rajath Karangara and Otilia Manta (2024), *Cybersecurity and Data Privacy in FinTech*, emphasized that protecting customer data has become a major concern with the widespread adoption of digital financial platforms. The authors concluded that strong cybersecurity practices and effective data protection measures are essential for maintaining user trust and ensuring secure financial services.

10. Fatmir Basholli, Davron A. Juraev, and Khojiakbar Egamberdiev (2024), *Framework, Tools and Challenges in Cyber Security*, reviewed various cybersecurity frameworks and security tools. The study explained key cybersecurity functions, including identification, protection, detection, response, and recovery. It also highlighted the importance of tools such as firewalls, antivirus software, and penetration testing while discussing emerging threats related to cloud computing, artificial intelligence, IoT, and ransomware.

11. Adebayo Y. Balogun, Kingsley Nana Peprah, Solomon Olaniyi Martins, Stacey Obielu, Job O. Adegede, Isyaku Abdullahi Odoguje, and Ebuka Mmaduekwe (2024), *Cybersecurity in Mobile FinTech Applications: Addressing the Unique Challenges of Securing User Data*, focused on cybersecurity challenges in mobile FinTech applications. The study found that encryption, authentication mechanisms, and biometric technologies improve mobile security but also identified the need for greater attention to user behavior and real-time threat detection.

Statement of the problem

The use of financial technology (FinTech) has made digital financial services such as online banking, mobile payments, and digital wallets faster and more convenient. Yet however there is an increase of cyber security issues such as hacking, internet crime; identity theft & phishing scams. They will cause loss of money, decrease confidence among consumers for a service offered online. Therefore it aims at identifying some cyber threats associated with fintech; then propose measures for making online banking safe & secure.

objectives

- 1.To understand the concept of cybesecuity and fintech
- 2.To analyze the impact of cybersecurity on the growth of the digital economy
- 3.To examine the role of AI, blockchain, and biometric authentication to protect online frauds and financial losses.
- 4.

III. RESEARCH METHADOOGY

Data Source: Primary Data.

Data Collection Method :Structured Questionnaire (Google Forms).

Users of UPI, mobile banking, digital wallets, and internet banking.

Study Area: Ballari

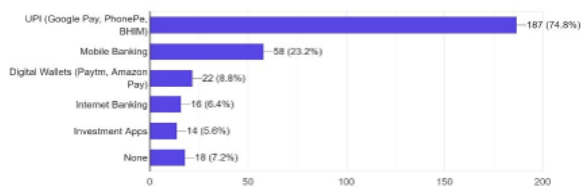
Sampling Technique: Convenience Sampling

Sample Size: 250 respondents

DATA ANALYSIS AND INTERPRETATION

5. Which FinTech services do you use most frequently?

250 responses

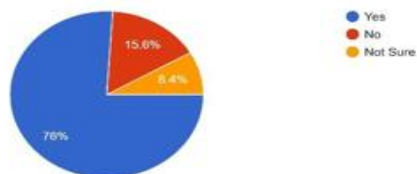


Interpretation

The chart shows that mobile wallets are the most frequently used FinTech service, with 74.4% of respondents choosing them. Digital wallets (such as Paytm and PhonePe) are the second most popular, used by 32.2% of respondents. A smaller number of participants use peer-to-peer (P2P) payments, internet banking, investment apps, and loans. This indicates that respondents mainly prefer simple and convenient digital payment methods for their daily transactions

7.Are you aware of cybersecurity threats in online financial transactions?

250 responses



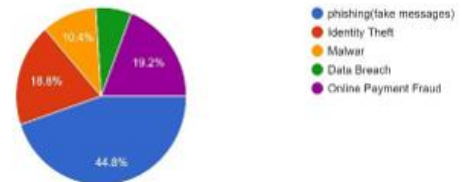
Interpretation:

A total of 76% of respondents stated that they are aware of cybersecurity threats in online financial

transactions. Meanwhile, 15.6% reported that they are not aware, and 8.4% were unsure. The findings suggest a high level of cybersecurity awareness among users, although a small section still requires greater awareness and education.

8. Which cybersecurity threat concerns you the most?

250 responses

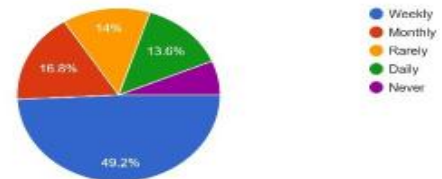


Interpretation:

Phishing was identified as the biggest cybersecurity concern by 44.8% of respondents. Online payment fraud ranked second with 19.2%, followed closely by identity theft at 18.8%. Malware accounted for 10.4%, while data breaches were reported by 6.8%. These results indicate that phishing and payment-related fraud are the primary cybersecurity concerns among digital users.

9.How often do you use digital payment services?

250 responses

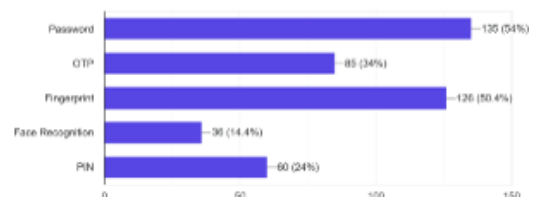


Interpretation:

Nearly half of the respondents (49.2%) use digital payment services weekly. Monthly usage was reported by 16.8%, while 14% use them rarely and 13.6% access them daily. Only 6.4% indicated that they never use digital payment services. The findings show that digital payment platforms are widely used, with weekly transactions being the most common pattern.

10.Which security feature do you use most often?(select more than one)

250 responses

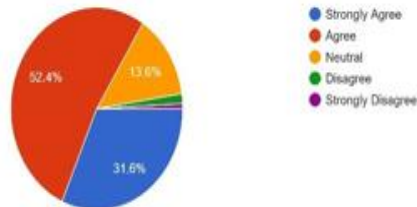


Interpretation

The chart shows that passwords (54%) are the most commonly used security feature among respondents. Fingerprint authentication (50.4%) is also widely

preferred, indicating the growing adoption of biometric security. OTP (34%) and PIN (24%) are used by a moderate number of users for transaction verification. Face recognition (14.4%) is the least preferred security feature. Overall, the findings suggest that respondents rely mainly on passwords and fingerprint authentication to secure their digital payment accounts.

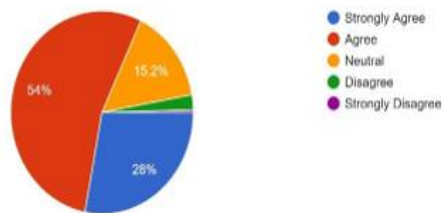
11. Do you believe cybersecurity is essential for the growth of the digital economy?
250 responses



Interpretation

A majority of the respondents agreed (52.4%) that cybersecurity is essential for the growth of the digital economy, while 31.6% strongly agreed with this view. In addition, 13.6% remained neutral, whereas only 1.6% disagreed and 0.8% strongly disagreed. These findings indicate that respondents have a positive perception of the importance of cybersecurity in promoting trust and supporting the growth of the digital economy.

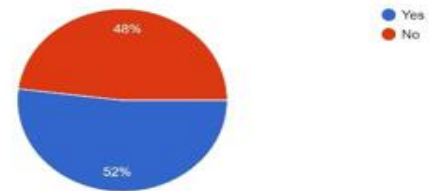
12. Does strong cybersecurity increase your trust in digital payment platforms?
250 responses



Interpretation

The chart indicates that 54% of respondents agree and 28% strongly agree that strong cybersecurity increases their trust in digital payment platforms. 15.2% remain neutral, while only a very small percentage disagree or strongly disagree. This shows that most users believe cybersecurity plays a key role in building confidence in digital transactions. Overall, effective security measures positively influence users' trust and encourage the use of digital payment services.

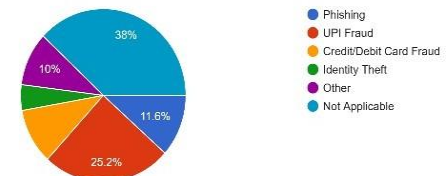
13. Have you ever experienced online financial fraud?
250 responses



Interpretation

Among the respondents, 52% reported that they had experienced online financial fraud, while 48% stated that they had not faced such incidents. This indicates that online financial fraud has affected a significant proportion of digital payment users. The findings highlight the need for stronger cybersecurity measures and greater user awareness to reduce the risk of online financial fraud.

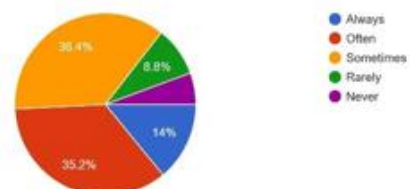
14. If yes, what type of fraud did you experience?
250 responses



Interpretation

The chart shows that phishing (38%) is the most commonly experienced type of online fraud among respondents. UPI fraud (25.2%) is the second most reported issue, highlighting the risks associated with digital payment systems. Credit/Debit card fraud (10%), identity theft (5.2%), and other frauds (10%) were reported by fewer respondents. 11.6% selected Not Applicable, indicating they had not experienced any fraud. Overall, the findings emphasize that phishing and UPI-related scams are the major cybersecurity threats faced by digital payment users.

15. Do cybersecurity concerns affect your willingness to use FinTech services?
250 responses



Interpretation

The findings indicate that cybersecurity concerns significantly influence respondents' willingness to use FinTech services. 36.4% stated that such

concerns sometimes affect their decision, while 35.2% reported they are often affected. Additionally, 14% always consider cybersecurity before using FinTech services. In contrast, 8.8% said these concerns rarely affect them, and 5.6% indicated they are never influenced. This highlights the importance of strong cybersecurity measures in building user trust.

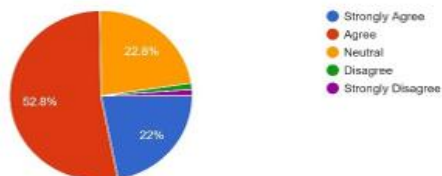
16. Which technology do you think is most effective in preventing online fraud?
250 responses



Interpretation

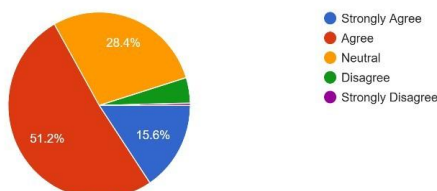
The results show that Artificial Intelligence (AI) (27%) is considered the most effective technology for preventing online fraud, followed by Biometric Authentication (26%) and Blockchain (24.8%). Multi-Factor Authentication (12.8%) also received notable support, while 14.4% of respondents were not sure. Overall, the findings reflect a positive perception of advanced technologies in enhancing cybersecurity and fraud prevention.

20. Do you think biometric authentication is more secure than passwords?
250 responses



The findings show that respondents generally believe biometric authentication is more secure than traditional passwords. A majority (52.8%) agreed with the statement, while 22% strongly agreed, indicating high confidence in biometric security. Additionally, 22.8% remained neutral, suggesting some uncertainty. Only 1.2% disagreed and 1.2% strongly disagreed, reflecting minimal opposition to the use of biometric authentication as a secure authentication method.

17. Do you think AI can detect fraudulent financial transactions effectively?
250 responses



Interpretation

The findings reveal that respondents have a positive perception of AI's ability to detect fraudulent financial transactions. 51.2% agreed and 15.6% strongly agreed that AI can effectively identify fraud. Meanwhile, 28.4% remained neutral, whereas only 4% disagreed and 0.8% strongly disagreed. This suggests growing confidence in AI as a reliable tool for financial fraud detection.

IV. FINDINGS

1. The study found that young adults (53.6%) are the major users of FinTech services, indicating that digital financial platforms are most popular among the 21–30 years age group.
2. The study reveals that 66.8% of respondents are familiar with FinTech, showing a good level of awareness about digital financial services.
3. The findings show that 74.4% of respondents mainly use mobile wallets and digital payment applications, making them the most preferred FinTech service.
4. The study found that 55% of respondents have experienced online financial fraud, indicating the need for strong cybersecurity measures and user awareness.
5. 57.2% of respondents agreed and 13.2% strongly agreed that blockchain improves digital transaction security, showing a positive opinion about blockchain.
6. 59.2% of respondents use fingerprint authentication, while 29.2% use face recognition, indicating that fingerprint is the most preferred biometric method.

V. CONCLUSION

The study concludes that FinTech has significantly contributed to the growth of the digital economy by making financial services more accessible, efficient, and convenient. At the same time, the increasing use of digital financial platforms has created new cybersecurity challenges that require continuous attention. The adoption of advanced security technologies, combined with user awareness and effective cybersecurity practices, is essential for protecting digital transactions and maintaining

consumer trust. Strengthening cybersecurity will support the sustainable growth of FinTech and ensure a secure digital financial ecosystem

REFERENCES

- [1] Faheem Ashraf and Sadi Badi (2025), in Cyber Risk and Data Privacy in FinTech: Strengthening Fraud Detection, Financial Institutions Security, and Regulatory Compliance, explained that FinTech has transformed financial services by making them faster and more accessible... Source: ResearchGate preprint (DOI: 10.13140/RG.2.2.22602.48327).
- [2] Souran, M. (2025). Cybersecurity Challenges and Strategic Defenses in FinTech: A Review of Emerging Threats and Mitigation Frameworks. In Proceedings of the 3rd International Conference on Cyber Resilience (ICCR 2025). IEEE. ISBN: 979-8-3315-5553-5. DOI: 10.1109/ICCR67387.2025.11292141.
- [3] Adetunji Paul Adejumo and Chinonso Peter Ogburie (2025), in The Role of Cybersecurity in Safeguarding Finance in a Digital Era, discussed the critical role of cybersecurity in protecting financial institutions... Published in: World Journal of Advanced Research and Reviews, 25(3), 1542–1556. DOI:10.30574/wjarr.2025.25.3.0909.
- [4] Muhammad Danish & Rohit Donni (2025). Cybersecurity Challenges in Digital Services: Managing Risk in a Rapidly Evolving FinTech Landscape https://doi.org/10.1007/978-3-030-64682-3_6
- [5] Ashish Juneja (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. Journal of Technology Innovations and Energy, Vol. 3, Issue 2, May 2024. ISSN:2957-8809. DOI: 10.56556/jtie.v3i2.907.
- [6] Adeyemi Akinyemi (2024). Cybersecurity in FinTech and Digital Payment Systems Multidisciplinary Innovations & Research Analysis, Vol. V, Issue IV (2024), pp. 84–99. ResearchGate full text available.
- [7] Paulin K. Kamuangu (2024). A Review on Cybersecurity in FinTech: Threats, Solutions, and Future Trends Journal of Economics, Finance and Accounting Studies, 6(1), pp. 47–53, ISSN 2709-0809, DOI: 10.32996/JEFAS.2024.6.1.5. ResearchGate full text available.
- [8] Rajath Karangara & Otilia Manta (2024). Cybersecurity and Data Privacy in FinTech <https://scholar.google.com/scholar>
- [9] Fatmir Basholli, Davron A. Juraev, and Khojiakbar Egamberdiev (2024), in Framework, Tools and Challenges in Cyber Security, <https://scholar.google.com/scholar>
- [10] Adebayo Y. Balogun et al. (2024). Cybersecurity in Mobile FinTech Applications: Addressing the Unique Challenges of Securing User Data World Journal of Advanced Research and Reviews, 23(2), pp. 2704–2710, DOI: 10.30574/wjarr.2024.23.2.2635.
- [11] Emmanuel Eturpa Salami et al. (2023). Systematic Literature Review on Cyber Insecurity Impact on African Economy Vol. 04, Issue 07, pp.5926-5931, July, 2023 Available online at <http://www.scienceijsar.com> ISSN: 2582-6425
- [12] Xiuli Chen et al. (2023). The Potential of the Digital Economy: A Comparative Assessment of Key Countries' Cybersecurity International Journal of Education and Humanities ISSN: 2770-6702 | Vol. 11, No. 1, 2023
- [13] Diptiben Ghelani et al. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banki American Journal of Computer Science and Technology doi: 10.11648/ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)
- [14] Radoica Luburić & Novak Fabris (2022). FinTech, Risk-Based Thinking and Cyber Risk Journal of Central Banking Theory and Practice, 2022, 2, pp. 27-53
- [15] Mamoon Humayun et al. (2021). Industry 4.0 and Cyber Security Issues and Challenges https://doi.org/10.1007/978-3-030-64682-3_6
- [16] Narcisa Roxana Moşteanu (2020), Challenges for Organizational Structure and Design as a Result of Digitalization and Cybersecurity, <https://doi.org/10.4018/IJBSA.2020040103>
- [17] Ademola Adeyoju (2019), Cybercrime and Cybersecurity: FinTech's Greatest Challenges, <https://scholar.google.com/scholar>
- [18] Faya Moses and Nnubia Ogbuefi (2019), Cybersecurity in the Age of FinTech and Digital Business, SSRN:

<https://ssrn.com/abstract=3606866>

- [19] Mario Spremic and Alen Simunic (2018),
Cyber Security Challenges in Digital Economy,
<https://scholar.google.com/scholar>
- [20] G. Nikhita Reddy and G. J. Ugander Reddy
(2014), A Study of Cyber Security Challenges
and Its Emerging Trends on Latest
Technologies, <https://scholar.google.com/scholar>