Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P.517-524 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

A Comprehensive Study on Security Measures and Consumer Awareness with Special Reference to UPI in India

Aniket Swaraj and Ayush Bohara

SIES College of Commerce & Economics (Autonomous), Mumbai, India
anikets.sies.edu.in

How to cite this article: Aniket Swaraj, Ayush Bohara (2024). A Comprehensive Study on Security Measures and Consumer Awareness with Special Reference to Upi in India *Library Progress International,* 44(3), 517-524.

ABSTRACT

The exponential surge of the Unified Payments Interface (UPI) in India has transformed digital transactions yet unveiled a realm of scams and frauds due to inadequate consumer education. The current body of literature comprehensively addresses the technological progress of UPI. This paper addresses critical lacunae in existing literature. Firstly, it illuminates the necessity of comprehensively exploring user security awareness amidst discussions of technological advancement. Secondly, it underscores the imperative of understanding user responses to financial malfeasance to fortify support systems. Lastly, it identifies a gap in integrating discussions on UPI's technological prowess with security measures. Through interdisciplinary inquiry, this research advocates for strategies to enhance consumer enlightenment, foster stakeholder collaboration, and iteratively refine UPI technologies. By encapsulating these insights, this study aims to not only deepen scholarly understanding but also catalyse practical measures toward fortifying the digital payment ecosystem against emerging threats.

Keywords: Fintech, E-Banking, UPI, Financial Cyber Security, Data Privacy.

INTRODUCTION

India is progressively advancing within the fintech growth trajectory, primarily attributed to its resilient fintech ecosystem, wherein numerous participants demonstrate increased support, both in terms of financial contributions and the development of technological and business acumen. A noteworthy facet of the nation's appeal lies in its robust talent pipeline, yielding a cost-effective and readily employable IT workforce.

However, impediments hindering widespread digital media adoption in India include the scarcity of reliable consumer information and inadequacies in the digital and technological infrastructure.

The burgeoning expansion of this industry is propelled by enhanced collaboration among market participants, fostering the utilisation and exchange of knowledge and expertise. A pivotal element for further advancement is the establishment of a cohesive fintech ecosystem characterised by 100% digital infrastructure penetration and impartial incubation support.

In recent years, the intersection of financial technology (Fintech) and electronic banking (E-Banking) has revolutionised the landscape of digital transactions. With the rapid adoption of technologies like Unified Payments Interface (UPI), the financial sector has witnessed unprecedented growth, offering users seamless and efficient methods of conducting transactions. However, this digital transformation has brought forth critical challenges, prominently centred around cyber security and data privacy. As financial activities increasingly migrate to online platforms, the vulnerability to cyber threats becomes a paramount concern. This paper delves into the multifaceted dimensions of Fintech, E-Banking, UPI, Cyber Security, and Data Privacy, aiming to comprehensively assess the current scenario, consumer awareness, and propose pragmatic recommendations. The evolving nature of these domains necessitates a thorough exploration to ensure the security and trustworthiness of digital financial transactions in the contemporary era.

LITERATURE REVIEW

Gai , K., Qiu , M., Sun , X., & Zhao , H. (2017) in their paper titled, ”Security and Privacy Issues: A Survey on FinTech” have produced a survey of FinTech by collecting and reviewing contemporary achievements in

security and privacy issues of the financial industry.

Stewart, H., & Jürjens , J. (2018) in their paper titled, " Data security and consumer trust in FinTech innovation in Germany" have identified the advancement of mobile devices and their usage have increased the uptake of financial technology (FinTech) innovation in Germany.

Hernández, E., Öztürk, M., Sittón , I., & Rodríguez , S. (2019)in their paper titled, " Data Protection on Fintech Platforms" look at the evolution of computer security in the field of Fintech due to the security level that it requires. In addition, it examines the solution techniques for data storage issues in cloud security and encryption methods that assure data protection. Also, the European Union's data protection regulation is considered.

Gai , K., Qiu , M., & Sun , X. (2019)in their paper titled, " A survey on FinTech.

Vijai, C. (2019). Fintech in India – Opportunities and Challenges"aims to produce a survey of FinTech by collecting and reviewing contemporary achievements in security and privacy issues of the financial industry in India,,

Mehrban, S., & Hussain, M. (2020) in their paper titled, " Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges" provides a comprehensive survey of FinTech by reviewing the most recent as well as anticipated financial industry privacy and security issues.

Alekseenko, A. P. (2022) in their paper titled, "Privacy, Data Protection, and Public Interest Considerations for Fintech" analyses the challenges caused by Fintech with regard to data privacy regulation. It is concluded that a model for an international legal framework on data privacy is needed. It could harmonise the different approaches of governments and standardise their policy for Fintech.

Dash, B., Sharma, P., & Ali, A. (2023) in their paper titled, " Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech." effectively describes the issue of federated learning for confidentiality. It describes the overall process associated with its development and some of the contributions it has achieved. The widespread application of federated learning in FinTech is showcased, and why federated learning is essential for overall growth in FinTech.

Narayan, A. (2023) in their paper titled, " Is your Data Safe with Fintech? An Analysis of India's Financial Data Protection Framework using GDPR Principles" examines the data protection framework for fintech companies in India through the lens of the General Data Protection Regulation (GDPR) implemented by the European Union. By analysing key GDPR principles such as accuracy, purpose limitation, accountability, storage limitation, data security, and lawfulness, the paper identifies gaps in India's data protection regulations and proposes potential solutions.

Rastogi, A. (2023) in their paper titled, "Impact of India's Data Protection Bill on Digital Platform Businesses" understands the impact this bill may have on platform businesses once the Data Protection Bill goes live and recommends actions and priorities to minimise business impacts for these platforms.

RESEARCHGAP

1. Insufficient Attention to Security Awareness and Precautions:
- The existing body of research literature on UPI primarily concentrates on technological developments and their transformational potential, but it does not thoroughly examine user security awareness. The present study highlights a significant gap in academic research with respect to the awareness, preventive measures, and proactive approaches that are necessary to safeguard consumers from potential security risks and financial fraud.

2. Unexplored User Responses to Financial Fraud:
- Although research on UPI transactions have acknowledged the presence of security risks, they have not been able to fully comprehend and record the behaviors and reactions of individual users when they have come across a financial fraud incidence. In order to create inclusive policies and support systems, it is essential to analyze the user-centric perspective in handling such occurrences.

3. Incomplete Integration of Security Measures into UPI Discussions:
- The literature assessment highlights a propensity to exclude careful consideration of security measures from conversations on UPI's technological innovations. In order to have a thorough grasp of UPI, there is a research gap that needs to be filled, as this study demonstrates. By incorporating security concerns into the main conversation about UPI adoption and usage, this integration guarantees that security concerns are not handled as incidental elements.

OBJECTIVES

1. **Evaluating Consumer Awareness and Perception**: Examine the degree of knowledge and understanding

among consumers about cybersecurity risks related to online financial transactions, with a focus on the contribution of education and communication to raising consumer awareness.

2. **Analysing Efficacy of Implemented Security Measures**: Examine the efficacy of security measures used by Fintech companies, evaluating their capacity to reduce risks and foster consumer trust, and pinpoint any weaknesses or opportunities for enhancement in the current security frameworks.

3. **Proposing Actionable Recommendations**: Assist Fintech businesses, regulators, and legislators in strengthening the entire security posture of online payments and banking, guaranteeing a stable and reliable ecosystem for customers, by offering practical and context-specific solutions.

RESEARCH METHODOLOGY

This study uses an exploratory methodology to look into a number of topics inside the UPI framework. The major goal of the survey-based methodology, which uses Google Forms for Convenient Sampling to disseminate surveys, is to thoroughly analyse consumer behaviour in the UPI sector. Evaluating customer perception and understanding of cybersecurity concerns related to online financial transactions, assessing the effectiveness of security measures put in place by Fintech companies, and making practical recommendations are the specific goals. The aforementioned aims are intended to provide significant insights into the UPI landscape. Specifically, they highlight the influence of education, communication, and security frameworks on consumer behaviour and the development of a reliable and secure online payment ecosystem. A total of 201 responses were collected from the respondents.

DATA ANALYSIS & FINDINGS:

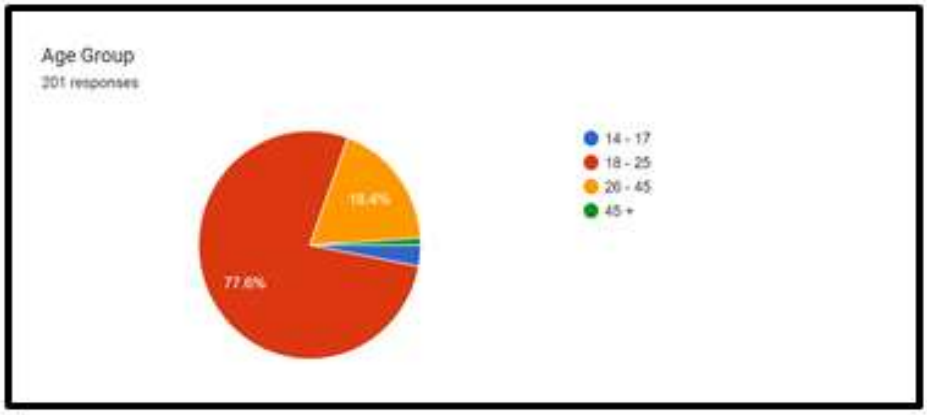

Illustration 1

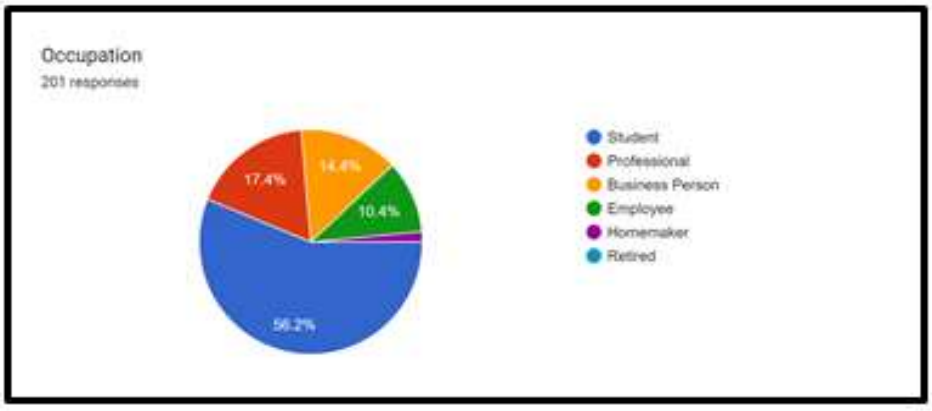

Illustration 2

The illustrations collectively depict a comprehensive profile of the respondents. In Illustration 1, the age distribution is highlighted, with a significant 77.6% falling within the 18-25 age range, followed by 18.4% in the 25-45 age group. Illustration 2 delves into their occupations, revealing that 56.2% identify as students, 17.4% as professionals, 14.4% as business persons, and 10.4% as employees. This combined overview underscores the diverse demographic characteristics, encompassing both age and occupational backgrounds of the surveyed participants.

Illustration 3

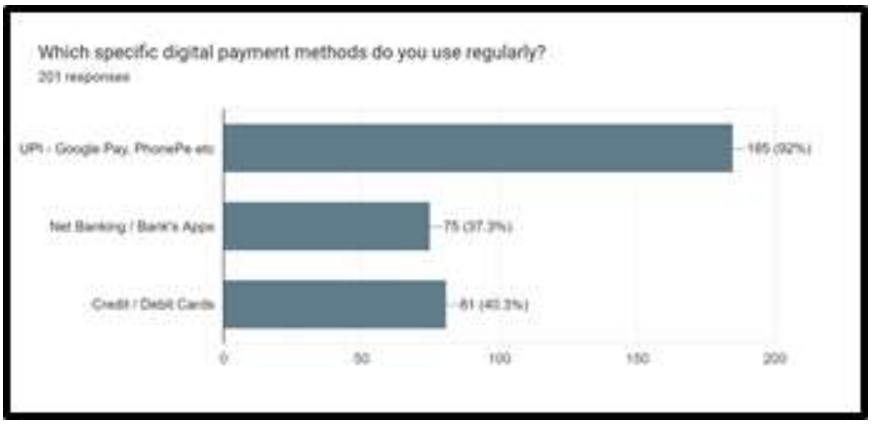

Illustration 4

Illustrations 3 and 4 provide insights into the usage patterns of UPI users. In Illustration 3, it is evident that 45.3% of respondents actively participate in financial transactions on a daily basis, with an additional 37.8% engaging in these transactions weekly. Illustration 4 sheds light on the preferred UPI platforms, indicating that a substantial number of respondents favour platforms like Google Pay, PhonePe, and Paytm. Credit and debit cards also play a significant role in user preferences, followed by net banking. This dual presentation offers a nuanced understanding of both transaction frequency and the popularity of various UPI platforms among the surveyed participants.

Illustration 5 delves into respondents' awareness regarding the storage practices of these platforms. A significant finding is that 54.2% of individuals express no awareness about how their data is stored or utilised. In contrast, 26.4% affirm their awareness, while 19.4% remain uncertain. The notable concern arises from the segment of respondents who lack awareness or are unsure about data storage Practices,yet continue to use the apps and services. This underscores a potential gap in user understanding and highlights the importance of addressing information transparency in digital platforms.

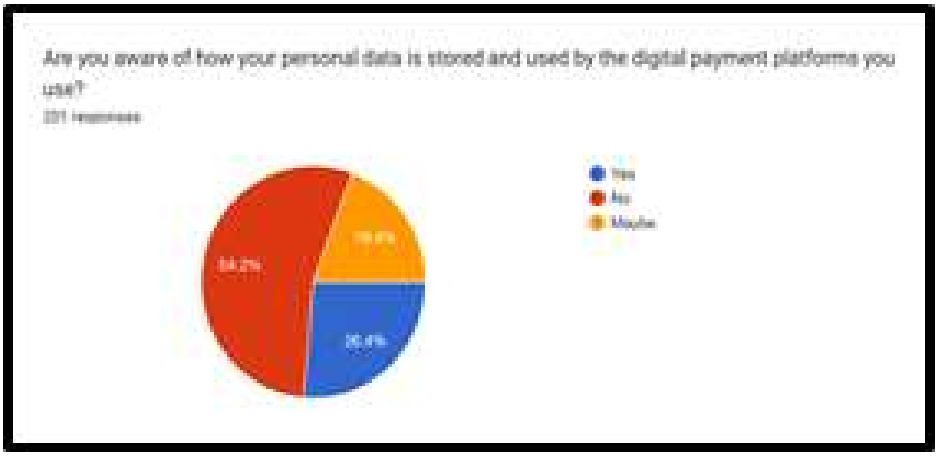

Illustration 5

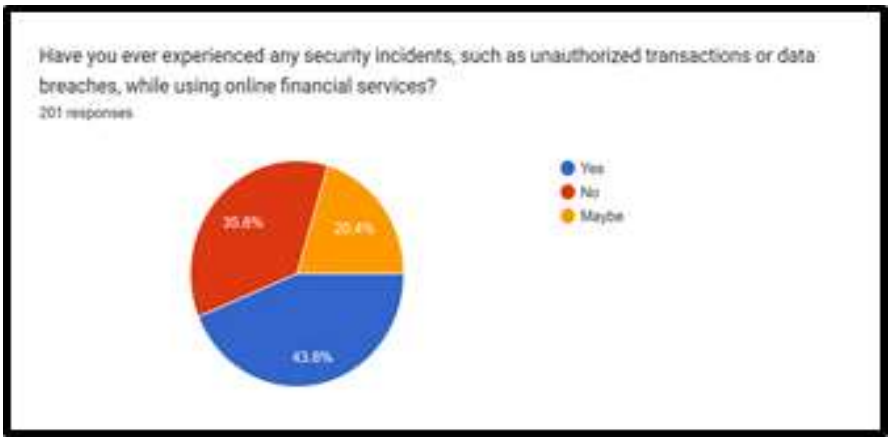

Illustration 6

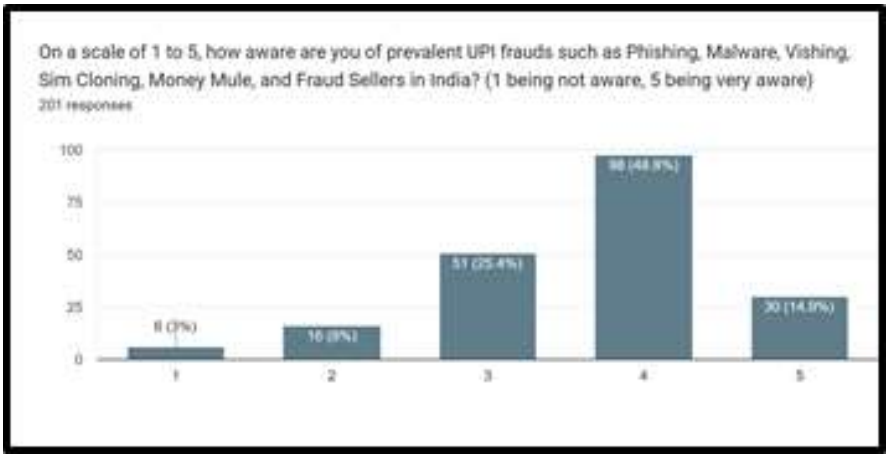

Illustration 7

Illustrations 6 and 7 shed light on respondents' incidental experiences. Illustration 6 reveals that a significant 48.8% of respondents have encountered a security breach or a similar incident concerning financial payments, while an additional 20.4% express uncertainty (possibly indicating a lack of awareness or education to identify such breaches). On the other hand, Illustration 7 indicates that a majority of respondents believe they are aware of online threats such as phishing and vishing. These findings underscore the prevalence of security incidents in the digital financial landscape and the need for enhanced education and awareness programs to empower users in recognizing and addressing potential threats.

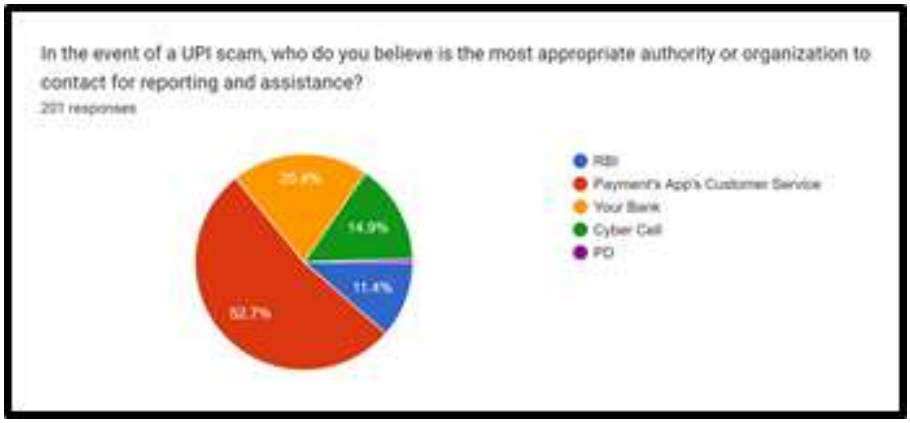

Illustration 8

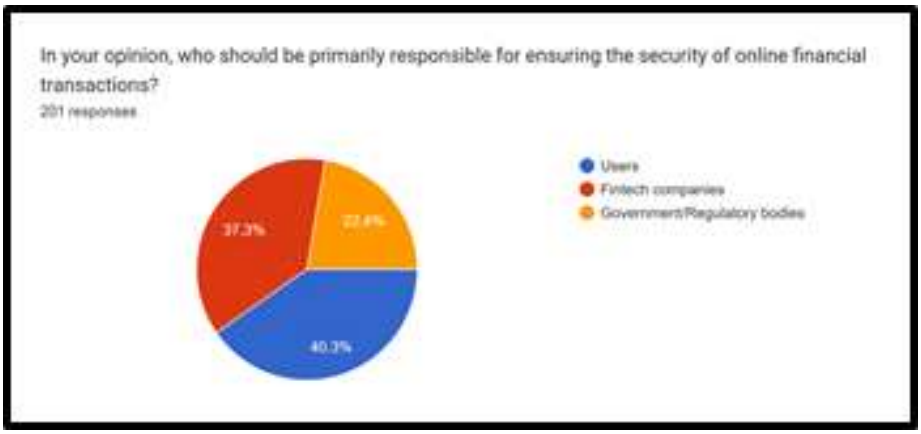

Illustration 9

Illustrations 8 and 9 gauge consumer knowledge and awareness. Illustration 8 investigates respondents' understanding of the appropriate authority to report UPI fraud, revealing that only 20% of participants correctly identify their bank as the right entity. The majority of respondents express uncertainty about the reporting procedure. In contrast, Illustration 9 explores opinions on accountability for maintaining security, with a notable 40.3% of participants believing that users themselves should be held accountable. Others attribute responsibility to either fintech companies or regulatory bodies. These findings underscore potential gaps in consumer awareness regarding the reporting process and the perceived responsibilities in ensuring security within the UPI framework.

SECONDARY FINDINGS

India is the third-biggest fintech hotspot in the world, with more than 2100 companies residing in its vibrant ecosystem that have significantly changed the country's payment landscape in the past five years. Fintech adoption remained strong in 2019 despite the pandemic's hurdles, with a remarkable 87% consumer acceptance rate, highlighting the continued reliance on digital financial services. Fintech companies are especially noteworthy in South Asia, where traditional banks frequently create obstacles to credit availability. They use cutting-edge underwriting techniques to offer credit and resolve creditworthiness restrictions.

According to a Statista survey done in February 2021, there was a notable 70% increase in UPI transactions, indicating the growing popularity of digital payment systems. With its Payments Vision 2025, the Reserve Bank of India (RBI) emphasises this change even more. It lays out detailed plans to completely redesign the payments industry and promote the move towards digital adoption. With fintech becoming more and more common, the banking and financial industry will face more competition and innovation as these customer-focused companies prioritise flexibility and work to advance financial inclusion. Fintech companies have achieved a competitive advantage in the market by taking advantage of a more favourable regulatory framework as compared to traditional banks.

There is a catch to this rise in fintech popularity, though: widespread fraud. Although these organisations support financial inclusion, they also gather a tonne of sensitive personal data, such as health, gender, caste, and biometrics, in addition to financial data. Fintech companies unintentionally burden customers with significant burdens, requiring them to negotiate complex environments and protect themselves against fraudulent practices, despite the obvious benefits they offer. This highlights structural flaws in the digitization process, and more research on these issues confirms the main conclusions and clarifies the two sides of India's fintech revolution.

A number of new features and improvements have been added to the Unified Payments Interface (UPI) architecture by the National Payments Corporation of India (NPCI). The UPI-ATM capability is a noteworthy addition as it allows cash withdrawals through UPI-enabled interfaces while doing away with actual debit cards. Transaction security is ensured by one-time QR codes. Furthermore, tap-and-pay capabilities and higher transaction limits are now possible for offline UPI payments using UPI Lite X and NFC-based offline UPI payments. These features are especially helpful in places with spotty internet access.

In addition, the NPCI unveiled Hello UPI, which enables safe, AI-based chat payments that work with both smartphones and feature phones and initially support Hindi and English. The UPI Credit Line, which functions similarly to Buy Now Pay Later items and offers pre-approved credit limitations for completing payments even in the event that account balances are insufficient, is another noteworthy innovation. With cooperation from the NPCI, banks, and industry stakeholders, these improvements represent UPI 2.0's dedication to enhancing digital transaction efficiency, security, and accessibility. In order to utilize these functionalities, customers need to

confirm that their banks are UPI 2.0 member banks, which allows for a smooth integration into already-existing UPI applications.

SUGGESTIONS

A number of strategic recommendations are made in light of the research findings in order to address the important problems found in the UPI environment. Above all, it is critical to support consumer education programs and push for their full integration into current banking and financial literacy activities. These courses need to be specifically designed to tackle the unique difficulties and dangers posed by UPI transactions, guaranteeing that participants are knowledgeable about safe online conduct.

Moreover, one of the most important recommendations is to encourage cooperation between Fintech businesses and academic institutions. This collaboration has the potential to act as a bridge between consumer awareness and technology advancement. Together, workshops, webinars, and training campaigns can be arranged to equip consumers with the knowledge they need to successfully manage the complexities of UPI transactions.

Furthermore, the execution of creative awareness campaigns comes to light as a crucial tactic. By utilising a range of media platforms, these ads aim to draw in a broad audience of users by highlighting the importance of implementing secure UPI procedures and identifying possible signs of fraud. Such programs have the potential to be extremely important in fostering a generalised awareness of cybersecurity.

Furthermore, it is critical to support Fintech companies in integrating user-friendly security elements into UPI applications. In-app assistance, interactive lessons, and real-time warnings can all play a big part in warning users about possible dangers and providing them with useful advice on how to properly secure their transactions.

An additional important recommendation is to commit to ongoing enhancements to UPI security protocols. Fintech businesses and regulatory organisations should continue to be on the lookout for new dangers, integrate cutting-edge encryption solutions, and keep a step ahead of changing cyberthreats. Last but not least, putting in place government-led programs to raise cybersecurity and digital literacy awareness would offer a comprehensive and organised strategy for strengthening the UPI ecosystem. Stakeholders may work together to create an environment for UPI in India that is safer, more resilient, and easier to use by implementing these strategic actions.

CONCLUSION

Conclusively, this thorough analysis illuminates the revolutionary terrain of UPI in India, exposing not only its outstanding achievements but also the obstacles that come with swift innovation. Despite the unmatched ease that comes with the rise in UPI use, there is a serious problem with the widespread frauds and scams that result from a lack of consumer education. The results highlight the vital necessity of a balanced growth trajectory, where innovations—while ground-breaking—must be supported by substantial and continuous consumer awareness campaigns.

The success of UPI highlights how consumers are receptive to technology changes and highlights how important consumer education is to maintaining a safe and reliable digital financial ecosystem. The present study promotes a constructive collaboration between innovation and education, imploring interested parties to acknowledge the mutually beneficial association between the two. Moreover, it strengthens the idea that, despite their merits, the innovations of today should not stop there; rather, a dedication to ongoing development is necessary to bolster the robustness and security of UPI technologies. Through the adoption of an all-encompassing strategy, interested parties may guide the fintech scene in India toward a future in which consumer protection and technical advancement live side by side, empowering and inspiring people.

REFERENCES

Gai , K., Qiu , M., Sun , X., & Zhao , H. (2017). Security and Privacy Issues: A Survey on FinTech. *International Conference on Smart Computing and Communication*. https://doi.org/https://link.springer.com/chapter/10.1007/978-3-319-52015-5_24

Stewart, H., & Jürjens , J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*. https://doi.org/https://www.emerald.com/insight/content/doi/10.1108/ICS-06-2017-0039/full/html?fullSc=1

Hernández, E., Öztürk, M., Sittón , I., & Rodríguez , S. (2019). Data Protection on Fintech Platforms. *International Conference on Practical Applications of Agents and Multi-Agent Systems*. https://doi.org/https://link.springer.com/chapter/10.1007/978-3-030-24299-2_19

Gai , K., Qiu , M., & Sun , X. (2019). A survey on FinTech. *Journal of Network and Computer Applications*. https://doi.org/https://www.sciencedirect.com/science/article/abs/pii/S1084804517303247

Vijai, C. (2019). Fintech in India – Opportunities and Challenges. *SSRN*. https://doi.org/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354094

Mehrban, S., & Hussain, M. (2020). Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges. *IEEE Access*. https://doi.org/https://ieeexplore.ieee.org/abstract/document/8976098

Alekseenko, A. P. (2022). Privacy, Data Protection, and Public Interest Considerations for Fintech. *Global Perspectives in FinTech*. https://doi.org/https://link.springer.com/chapter/10.1007/978-3-031-11954-5_3

Dash, B., Sharma, P., & Ali, A. (2023). Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA), Vol.13, No.4, July 2022*. https://doi.org/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323967

Narayan, A. (2023). Is your Data Safe with Fintech? An Analysis of India's Financial Data Protection Framework using GDPR Principles. *SSRN*. https://doi.org/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4465239

Rastogi, A. (2023). Impact of India's Data Protection Bill on Digital Platform Businesses. *SSRN*. https://doi.org/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4574659