

**A
PROJECT REPORT
ON
“A STUDY ON USER PERCEPTION OF DATA PRIVACY
AND SECURITY IN FINTECH APPLICATIONS”**

SUBMITTED

To

CENTRE FOR ONLINE LEARNING

Dr. D. Y. PATIL VIDYAPEETH, PUNE



**IN PARTIAL FULFILMENT OF DEGREE OF
MASTER OF BUSINESS ADMINISTRATION**

BY

NAME OF THE STUDENT

PRN:

BATCH 2023-2025

**Dr. D.Y. Patil Vidyapeeth's
CENTRE FOR ONLINE LEARNING,
Sant Tukaram Nagar, Pune.**

CERTIFICATE

This is to certify that **Mr.** PRN - has completed his internship at **PB Fintech Limited** starting from 20/03/2025 to 27/04/2025.

His project work was a part of the MBA (ONLINE LEARNING)

The project is on “**A Study on User Perception of Data Privacy and Security in Fintech Applications**” which includes research as well as industry practices. He was very sincere and committed in all tasks.

Course Coordinator

Date -




To whomsoever it may concern

This is to certify that **Mr.** PRN - has completed his internship at **PB Fintech Limited** starting from 20/03/2025 to 27/04/2025.

His project work was a part of the MBA (ONLINE LEARNING)

The project is on “**A Study on User Perception of Data Privacy and Security in Fintech Applications**” which includes research as well as industry practices. He was very sincere and committed in all tasks.

The image shows a handwritten signature in blue ink over a circular blue stamp. The stamp contains the text 'PB Fintech Limited' around the top edge and 'Haryana 122001' around the bottom edge. Below the signature and stamp, the text 'Signature & Seal of Industry Guide' is written in blue.

Signature & Seal of Industry Guide

Plot 119, Sector 44, Gurugram, Haryana 122001

DECLARATION BY LEARNER

This is to declare that I have carried out this project work myself in part fulfillment of the M.B.A Program of Centre for Online Learning of Dr. D.Y. Patil Vidyapeeth's, Pune – 411018.

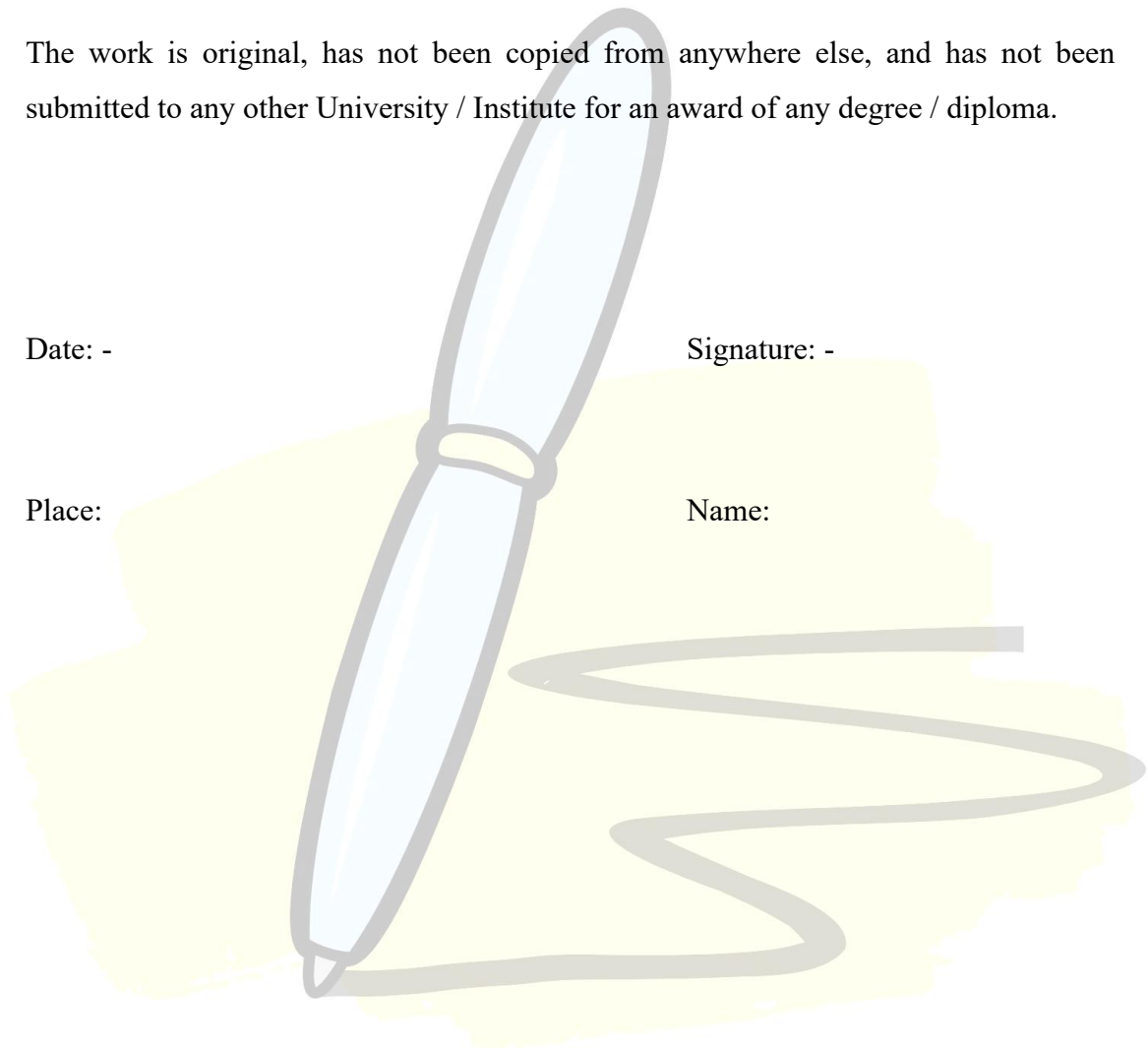
The work is original, has not been copied from anywhere else, and has not been submitted to any other University / Institute for an award of any degree / diploma.

Date: -

Signature: -

Place:

Name:



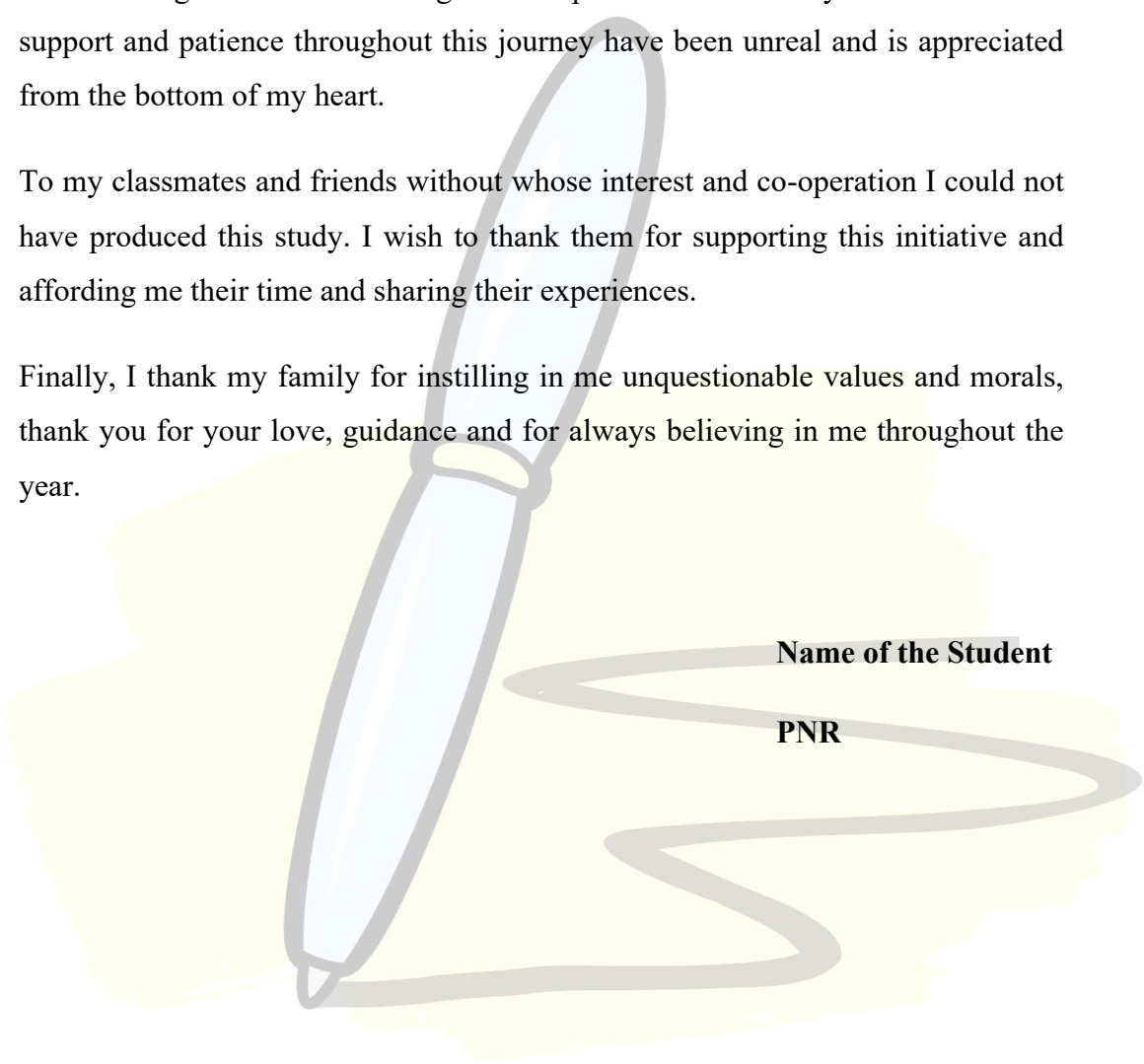
ACKNOWLEDGEMENT

First and foremost, I thank the Almighty God, for granting me the strength, health and courage to complete this arduous task.

A special thank you to my supervisor **Dr.** for his guidance, insight and encouragement in the writing and compilation of this study. Your invaluable support and patience throughout this journey have been unreal and is appreciated from the bottom of my heart.

To my classmates and friends without whose interest and co-operation I could not have produced this study. I wish to thank them for supporting this initiative and affording me their time and sharing their experiences.

Finally, I thank my family for instilling in me unquestionable values and morals, thank you for your love, guidance and for always believing in me throughout the year.



Name of the Student

PNR

TABLE OF CONTENT

Sr. No.	Item	Page No.
1	Executive Summary	1-2
2	Chapter 1: Introduction	3-26
3	Chapter 2: Literature Review	27-43
4	Chapter 3: Research methodology	44-45
5	Chapter 4: Data Analysis	46-69
6	Chapter 5: Findings, suggestions, recommendation	70-72
7	Chapter 6: Conclusion	73
8	Bibliography	74-78
9	Annexure	79-84
10	Scope for future study	85

EXECUTIVE SUMMARY

This research project titled “**A Study on User Perception of Data Privacy and Security in Fintech Applications**” explores the growing concern among users regarding the safety of their personal and financial information while using fintech platforms. As fintech has evolved to the point where people are using mobile wallets, online banking, investment platforms and payment gateways for everyday financial needs, it has changed how people relate to money. This digital convenience, however, carries significant risks—data breaches, unauthorized data sharing, little transparency about privacy practices—that have fueled significant anxiety around protecting user data.

The research was a descriptive study, comprising both qualitative and quantitative nature. Data collection was done via a structured Likert scale questionnaire administered to 100 fintech app users collected through convenient sampling. Supporting context was provided by secondary data drawn from reports, journals, and online sources. Patterns and insights were identified by analyzing data through percentage analysis made using tables and charts.

Overall, the findings show that although FinTech users tend to have high trust in the security capabilities of these applications; a major discrepancy in knowledge about privacy policies and sharing of third-party data still exists. Because of them, user confidence has turned around. Though, concern over unwanted use personal data and data security breaches persist. These concerns are truly interesting because, despite that, many users continued to use fintech apps regularly at least one or more times a month, selecting the convenience over caution. What's more is that when opting for fintech platforms, users seize on data securities reputation.

This result has been incorporated into the study and it is suggested that fintech companies should simplify their privacy policy, incorporate in app awareness features to educate users, and improve data handling practices ensured higher transparency. All this does not mean that you can ignore the issue of security and trust building — you should implement robust security protocols and clear communication in cases of incidents to promote user trust.

Finally, we conclude that data privacy and security are important drivers determining user behavior in the fintech landscape. While opinions towards fintech at the moment are slightly more positive, educating users to be more security minded and reinforcing security measures is going to be integral to maintaining growth and trust in the sector. This study offers a significant contribution toward understanding user expectations for fintech companies looking to some degree of regulatory compliance and their alignment with prevailing regulatory standards.



CHAPTER 1

INTRODUCTION

1.1. Introduction of the Study:

The digital age has transformed traditional financial services, reintroducing the market to financial technology (fintech) that changes the ways we manage, transfer and invest money. Online banking, peer to peer lending, and investing apps are quickly becoming part of daily financial activities and the popularity of mobile wallets has meant that the use of fintech apps is growing dramatically. For many, their convenience, speed and accessibility provided a gateway to everyone globally, attracted millions of users, inclusive of those ones had never guessed, to financial inclusion and personalized financial services at scale unparalleled. While this transformation is digital, it has also resulted in major data privacy and security concerns.

With an immense amount of personal and financial data at stake, data protection is now a critical element both for service providers and users alike when it comes to using the emerging fintech applications. As data breaches, phishing attacks, and unauthorized data sharing occur increasingly often, users are becoming more careful about how your info is collected, stored, and used. While many of the latest security advancements like encryption, biometric authentication, and secure cloud infrastructure are in place, user trust and awareness still persist.

In this study, user perception about data privacy and security in fintech is studied. It looks at how users judge safety of their information, what influences their trust, and how privacy worries affect their actions and choices. The study then analyzes user awareness, worries and contentment with current security measures to share insights on how fintech providers can enhance transparency, bolster user relations and support their rules with corresponding client objectives and regulatory precursors.

1.2. Background of the Study:



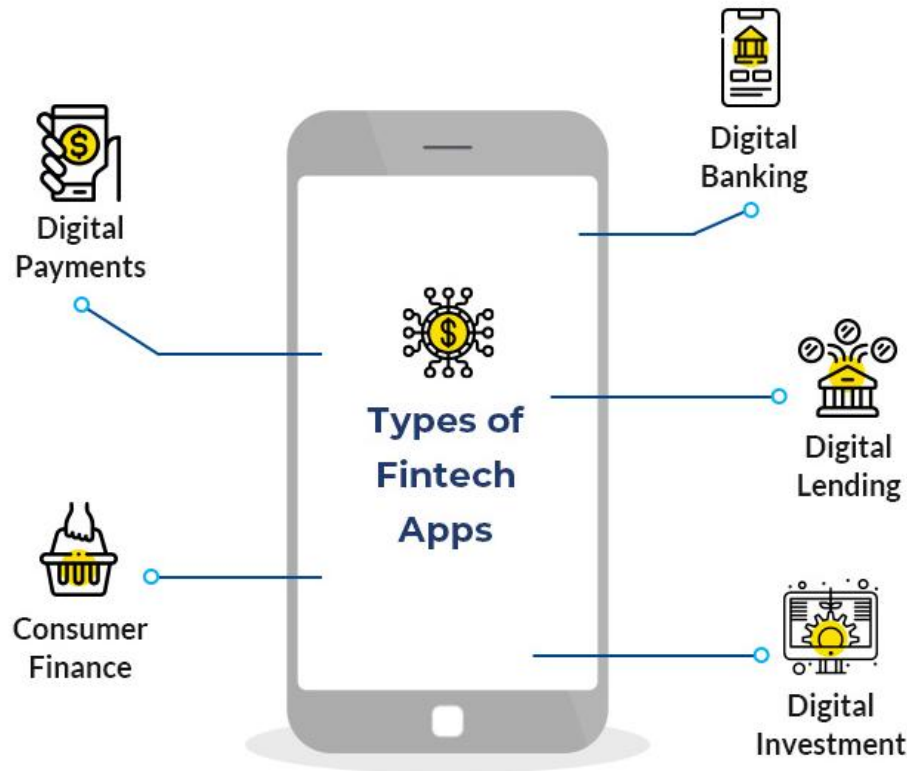
Overview of Fintech Applications

Fintech refers to any financial technology that will dramatically improve or redesign the delivery and use of financial services. Modern technologies like artificial intelligence, machine learning, big data, blockchain and mobile computing have been used to create efficient, accessible and user centric financial services — that's fintech. Primarily, these applications intend to make financial transactions more convenient, faster and cheaper as well as extending financial inclusion.

Fintech applications cover a wide range of services including digital banking, mobile wallets (e.g., Google Pay, PhonePe), peer-to-peer (P2P) lending platforms, investment and wealth management apps (e.g., Zerodha, Groww), personal finance trackers, crowdfunding platforms, robo-advisors, and insurance technology (insurtech). Many of these platforms are app-based, operating on smartphones, and are integrated with cloud services for real-time processing and data synchronization.

One of the core characteristics of fintech applications is their heavy reliance on user data, including personal identification details, financial behavior patterns, and transaction history. This data-centric approach allows for personalized services, improved credit scoring models, fraud detection, and predictive analytics. However, it also raises significant concerns related to data privacy, cybersecurity, and user consent, making the perception of security a critical factor in the adoption and continued use of fintech services.

Types of Fintech Apps found in the market today



The fintech (financial technology) industry has revolutionized how individuals and businesses manage money, offering convenience, speed, and accessibility through innovative digital solutions. From making seamless payments to managing investments, fintech apps cater to a wide range of financial needs. Below are some of the major types of fintech applications that are transforming the global financial landscape.

1. Digital Payments

Digital payment apps enable users to transfer money, make purchases, and pay bills instantly through mobile devices or online platforms. These apps eliminate the need for cash transactions and offer secure, real-time processing. Popular examples include mobile wallets, UPI-based apps, and contactless payment systems. Their convenience and security features have made them an essential part of everyday transactions.

2. Digital Banking

Digital banking apps provide users with a complete banking experience without visiting physical branches. Through these apps, customers can open accounts, check balances, transfer funds, deposit cheques, and access other banking services anytime. Many banks now operate entirely online, offering faster services and lower operational costs, while integrating advanced security measures such as biometric authentication.

3. Digital Lending

Digital lending platforms connect borrowers with lenders through an online interface, streamlining the loan approval and disbursement process. These apps use algorithms and data analytics to assess creditworthiness quickly, reducing paperwork and offering instant loan approvals. They cater to personal loans, business loans, and even microloans, making credit more accessible to a broader population.

4. Digital Investment

Digital investment apps allow users to invest in stocks, mutual funds, cryptocurrencies, and other assets directly from their smartphones. They often provide tools for portfolio tracking, market analysis, and automated investing (robo-advisors). By lowering entry barriers and offering fractional investment options, these apps encourage more people to participate in wealth-building activities.

5. Consumer Finance

Consumer finance apps focus on personal money management, helping users budget, track expenses, and improve their financial health. They may include features like bill reminders, credit score monitoring, and financial goal setting. Such apps empower users to make informed decisions, avoid debt traps, and achieve financial stability through better money management habits.

Functional Aspects of Fintech Applications

The functionality of fintech applications goes beyond digitizing financial services; it transforms how users interact with money, make decisions, and manage risks. These applications are built with user-centric features, robust infrastructure, and automated processes that deliver high performance, security, and convenience. Understanding the core functional aspects of fintech applications provides insights into how they improve financial inclusion, optimize user experience, and ensure operational reliability.

1. User Authentication and Onboarding

Fintech applications prioritize secure and seamless onboarding through digital KYC (Know Your Customer) and biometric authentication. Users can open accounts or register within minutes by uploading ID documents or using facial recognition and OTP-based verification. This functionality reduces paperwork and waiting time while ensuring compliance with regulatory norms.

2. Transaction Processing

One of the key functional aspects is real-time transaction processing, enabling instant payments, fund transfers, and settlements. This is achieved through integration with payment gateways, UPI networks, and core banking systems. The use of secure protocols and APIs ensures that transactions are both fast and tamper-proof.

3. Data Analytics and Personalization

Fintech platforms use data analytics to track user behavior, spending patterns, and preferences. This data is used to offer personalized insights, budgeting tips, credit score monitoring, and targeted product recommendations. AI-driven personalization improves customer engagement and satisfaction by offering relevant financial services at the right time.

4. Risk Assessment and Credit Scoring

Fintech apps employ alternative credit scoring models that analyze non-traditional data such as mobile usage, utility payments, and social behavior. These models are especially useful in assessing creditworthiness for customers without formal credit histories, thus promoting financial inclusion for underserved segments.

5. Security and Fraud Detection

Security features include end-to-end encryption, tokenization, multi-factor authentication, and real-time fraud monitoring. Many platforms also use AI to detect suspicious activity patterns, reduce false positives, and take proactive action against fraud. These measures ensure that sensitive user data and transactions are safeguarded.

6. Integration with Financial Ecosystems

Fintech apps often integrate with banks, insurance companies, investment platforms, and regulatory databases. This interoperability allows users to manage multiple financial activities—such as savings, loans, investments, and insurance—from a single platform. It also helps streamline services through a connected financial infrastructure.

7. User Interface and Experience (UI/UX)

An intuitive user interface and seamless user experience are central to fintech functionality. Features like dashboards, real-time notifications, chatbots, and voice commands are incorporated to enhance usability. Simple navigation and minimalistic designs ensure that users with varying levels of digital literacy can effectively use the applications.

8. Automation and Self-Service

Automation enables users to set recurring transactions, receive automated alerts, or invest using robo-advisors. This self-service model reduces dependence on customer support, saves time, and empowers users to manage their finances independently.

Technology Used in Ensuring Data Privacy and Security

In fintech applications, safeguarding user data is not only a legal requirement but also a cornerstone of building trust and ensuring user adoption. As these applications process vast amounts of sensitive financial and personal information, robust technological safeguards are vital. Fintech companies use a combination of advanced encryption, authentication methods, secure architectures, and real-time monitoring tools to protect data integrity, confidentiality, and availability. These technologies form the backbone of a secure fintech ecosystem.

1. End-to-End Encryption (E2EE)

Encryption is the fundamental layer of data protection used to secure data both in transit and at rest. End-to-end encryption ensures that only the sender and the intended recipient can access the information, rendering it unreadable to intermediaries or attackers. Fintech apps commonly implement AES-256 encryption, a military-grade standard, to secure financial transactions and user credentials.

2. Multi-Factor Authentication (MFA)

MFA enhances login security by requiring users to verify their identity through two or more credentials—typically a password, a smartphone-based OTP, or a biometric scan. This greatly reduces the chances of unauthorized access, especially in case of stolen or leaked passwords. Most fintech platforms mandate MFA for high-risk actions such as money transfers and account changes.

3. Tokenization

Tokenization replaces sensitive data (like card numbers or account details) with unique, non-sensitive equivalents called tokens. These tokens are meaningless outside the system, and actual data is securely stored in a centralized vault. This method is widely used in digital payments to prevent data breaches during transactions.

4. Biometric Authentication

Many fintech apps integrate biometric authentication features such as fingerprint scanning, facial recognition, and voice recognition for enhanced user verification. Biometrics are unique and hard to replicate, thus adding a strong layer of identity protection, especially in mobile fintech environments.

5. Secure Application Programming Interfaces (APIs)

Fintech apps rely heavily on APIs for connecting with banks, payment gateways, and third-party services. These APIs are secured using OAuth, SSL/TLS protocols, and access tokens to ensure that only authorized systems can communicate, thereby preventing data leaks and unauthorized integrations.

6. Artificial Intelligence (AI) for Threat Detection

AI-powered systems are used to monitor user behavior and transaction patterns in real-time to detect anomalies or suspicious activities. These systems can identify potential threats such as account takeovers, fraud attempts, or phishing attacks, allowing immediate intervention and mitigation.

7. Blockchain for Data Integrity and Transparency

Some fintech platforms utilize blockchain technology to ensure data immutability and transparency. In blockchain-based systems, each transaction is recorded in a decentralized ledger that cannot be tampered with, enhancing auditability and reducing the risk of data manipulation.

8. Cloud Security and Infrastructure Hardening

Many fintech services operate on cloud platforms. Providers implement virtual private clouds (VPCs), firewalls, intrusion detection systems (IDS), and regular vulnerability assessments to protect cloud-based data and applications. Role-based access control (RBAC) and encryption of backups further strengthen the infrastructure.

9. Privacy by Design and Data Minimization

Modern fintech applications follow the principle of “privacy by design,” embedding privacy controls in the architecture itself. This includes collecting only necessary data, providing clear consent options, and allowing users to control how their data is shared or deleted. It ensures compliance with data protection regulations and enhances user confidence.

Psychological Factors Influencing User Trust in Fintech Applications

Trust is a fundamental element that determines user adoption, retention, and reliance on fintech applications. While technological safeguards and regulatory compliance are crucial, the psychological perception of security and control plays a vital role in how users evaluate the safety and credibility of these platforms. Trust is shaped not only by system performance but also by individual experiences, cognitive biases, and emotional responses. Understanding these psychological factors helps fintech companies design more intuitive and trustworthy user experiences.

1. Perceived Control

Users are more likely to trust a fintech app when they feel in control of their personal data. Features like customizable privacy settings, clear consent prompts, and the ability to opt out of data sharing contribute to a stronger sense of control. When users perceive that they can manage how their information is collected and used, their trust in the platform increases significantly.

2. Transparency and Communication

Trust is built through honest and consistent communication. Fintech apps that provide transparent information about their data handling policies, security practices, and terms of service foster greater confidence. Users respond positively to simple, jargon-free disclosures about how their data is stored, processed, and protected.

3. Past Experience and Familiarity

Users who have had positive experiences with a particular app or brand are more likely to trust it again. Familiarity with app interfaces, smooth past transactions, and good customer service create a comfort zone that reinforces trust. Conversely, any prior data breach or poor service experience can lead to skepticism and decreased usage.

4. Risk Perception

Risk perception refers to a user's subjective judgment of the potential harm or vulnerability when using a fintech application. If users believe that the risks of financial loss, identity theft, or data misuse are high, they may avoid the app—even if it is objectively secure. Visual cues like padlock icons, security badges, and authentication prompts can help reduce perceived risk.

5. Brand Reputation and Social Influence

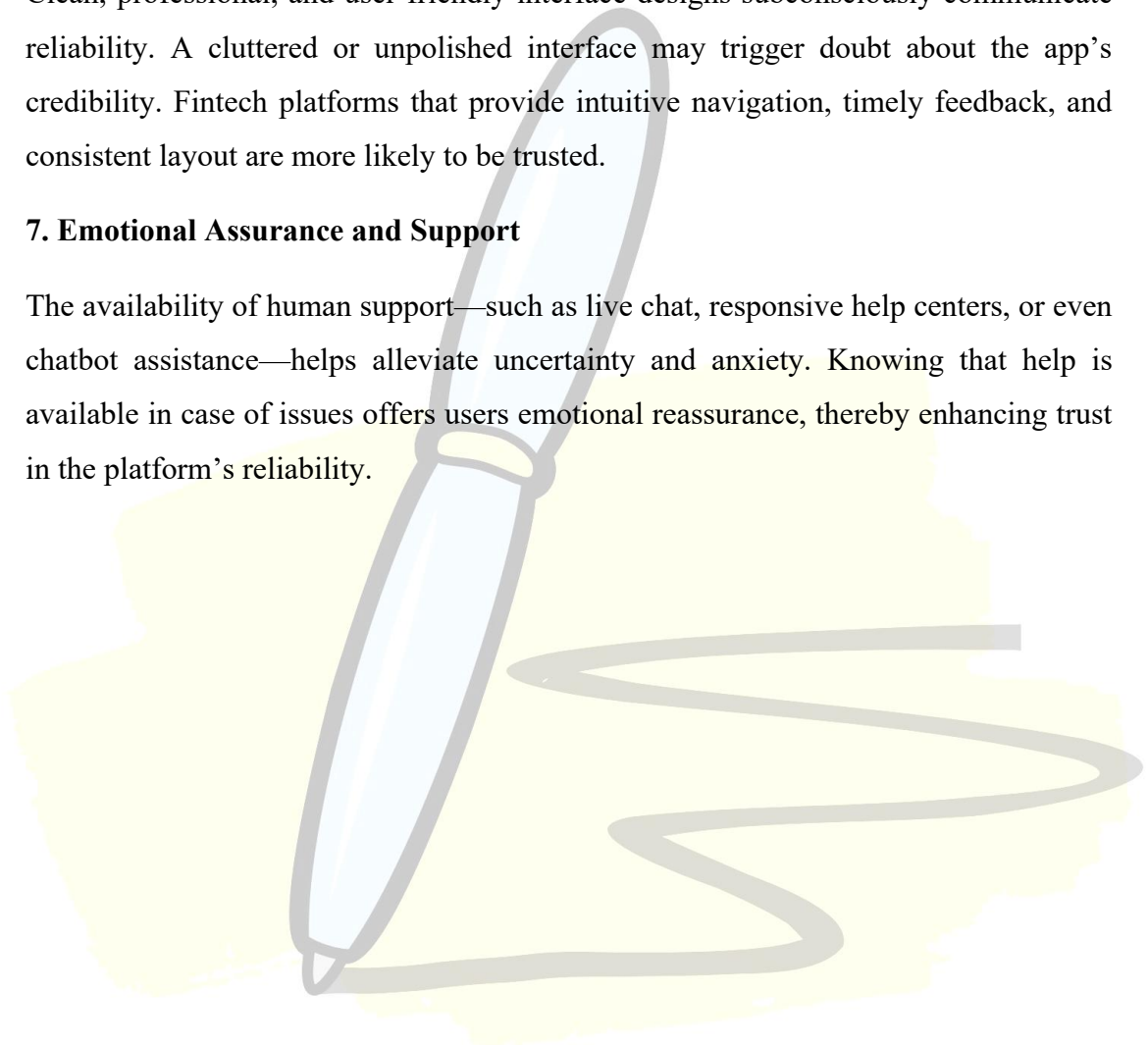
Users are influenced by brand image, media coverage, and peer recommendations. A strong, reputable brand is associated with higher trustworthiness, especially in financial matters. Additionally, hearing positive feedback or reviews from friends, family, or online communities can positively shape users' trust levels.

6. User Interface Design and Aesthetics

Clean, professional, and user-friendly interface designs subconsciously communicate reliability. A cluttered or unpolished interface may trigger doubt about the app's credibility. Fintech platforms that provide intuitive navigation, timely feedback, and consistent layout are more likely to be trusted.

7. Emotional Assurance and Support

The availability of human support—such as live chat, responsive help centers, or even chatbot assistance—helps alleviate uncertainty and anxiety. Knowing that help is available in case of issues offers users emotional reassurance, thereby enhancing trust in the platform's reliability.



Challenges in Implementing Data Security in Fintech

While fintech applications are designed to deliver fast, convenient, and innovative financial services, ensuring robust data security remains a critical challenge. As fintech platforms handle sensitive user information such as personal identity details, financial records, and transaction histories, they become prime targets for cyber threats. Despite advancements in encryption and threat detection technologies, several technical, regulatory, and user-related obstacles hinder the effective implementation of comprehensive data security frameworks in fintech.

1. Evolving Cyber Threats and Attack Vectors

Cybercriminals continuously adapt to emerging security technologies by developing new methods of attack such as phishing, ransomware, malware, and account takeovers. The dynamic nature of threats makes it difficult for fintech firms to maintain up-to-date defenses. A single successful breach can result in the exposure of millions of user records and irreparable damage to brand trust.

2. Complex Regulatory Compliance

Fintech platforms often operate across multiple jurisdictions, each with its own data protection laws (e.g., GDPR, India's DPDP Act, RBI cybersecurity guidelines). Ensuring compliance with all relevant regulations is time-consuming and requires constant monitoring and updates to policies and systems. Non-compliance can lead to legal penalties and loss of operating licenses.

3. Data Integration and Third-Party Risks

Fintech applications often integrate with banks, credit bureaus, and third-party APIs. Each integration point increases the risk of data leakage if the third party lacks adequate security measures. Ensuring security across the entire data ecosystem—including external partners—is a major challenge in maintaining end-to-end data protection.

4. Limited Cybersecurity Awareness Among Users

Many users are unaware of safe digital practices and may fall victim to social engineering or phishing attacks. Weak passwords, sharing OTPs, or using unsecured networks can compromise account security, even if the platform itself is secure. Educating users remains a critical yet under-addressed component of fintech security.

5. Budget Constraints for Startups and Small Players

Unlike large financial institutions, many fintech startups operate with limited resources. Implementing enterprise-grade security solutions such as intrusion detection systems, encryption infrastructure, and 24/7 threat monitoring can be costly. As a result, some smaller players may compromise on security in favor of faster development and market entry.

6. Balancing Security with User Experience

Implementing stringent security protocols like multi-step verification and frequent authentication checks can negatively impact user experience. Striking the right balance between strong security and ease of use is a constant struggle, as overly complex processes can lead to user drop-offs or dissatisfaction.

7. Insider Threats and Human Error

Data breaches are not always caused by external hackers; employees, developers, or contractors with system access can unintentionally or maliciously compromise data security. Managing internal access controls, conducting background checks, and providing employee training are essential but often overlooked aspects of fintech security management.

8. Inadequate Incident Response and Recovery Plans

Even with strong defenses, breaches can occur. However, many fintech firms lack well-defined incident response strategies. Without clear protocols for detection, containment, communication, and recovery, the impact of a data breach can be significantly amplified.

Impact of Data Privacy on User Adoption and Retention

In the digital finance landscape, data privacy is no longer just a compliance requirement—it is a critical factor influencing consumer behavior. As fintech applications increasingly rely on personal and financial data to deliver personalized services, users have become more aware and concerned about how their information is collected, stored, and used. The perception of strong data privacy directly affects users' willingness to adopt fintech platforms and their likelihood of continued usage over time. A breach of this trust can lead to user attrition, reputational damage, and business loss.

1. Influence on Initial Adoption Decisions

Data privacy concerns significantly shape a user's decision to try or install a fintech application. Users are more likely to adopt platforms that clearly communicate their privacy policies, provide options for consent, and minimize unnecessary data collection. Transparency about data practices at the onboarding stage builds user confidence and drives higher initial adoption rates.

2. Trust and Long-Term Engagement

Continued usage of fintech platforms is heavily dependent on sustained trust. When users feel that their sensitive information is safe and that the platform respects their privacy, they are more likely to return, engage, and explore additional services. This trust fosters brand loyalty, especially in segments like digital banking, investment apps, and insurance where long-term relationships are crucial.

3. Impact of Data Breaches on User Attrition

Data breaches—whether from cyberattacks or internal lapses—can severely damage user trust. Even a single privacy incident can lead to mass uninstallations, bad reviews, and negative word-of-mouth. Recovery from such events is difficult and often requires substantial investment in PR, compliance, and customer compensation.

4. Role in Differentiation and Competitive Advantage

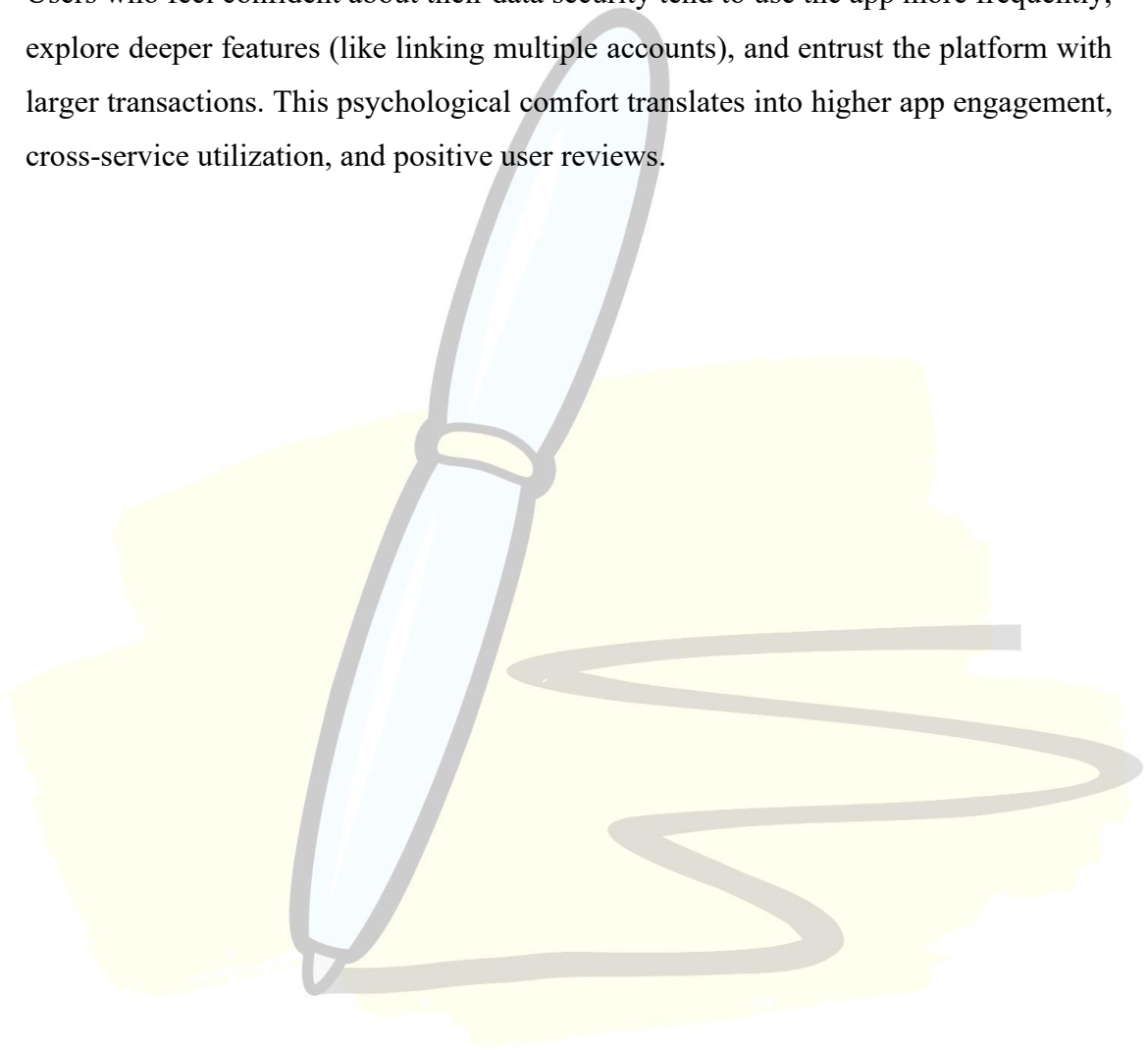
Fintech firms that adopt “privacy-first” strategies—such as data minimization, user-controlled privacy settings, and real-time privacy alerts—can use these as competitive differentiators. In a crowded market, strong data privacy practices can serve as a unique selling point that attracts privacy-conscious users.

5. Regulatory Alignment and User Perception

Platforms that align with global privacy standards (like GDPR, CCPA, or India's DPDP Act) are perceived as more trustworthy. Displaying compliance badges or certifications reassures users about the platform's credibility and dedication to safeguarding personal data, further improving adoption and retention.

6. Psychological Comfort and Usage Frequency

Users who feel confident about their data security tend to use the app more frequently, explore deeper features (like linking multiple accounts), and entrust the platform with larger transactions. This psychological comfort translates into higher app engagement, cross-service utilization, and positive user reviews.



Benefits of Technology-Driven Transparency in Fintech

Transparency is a key pillar of trust in financial services, especially in the fintech sector where users rely on digital platforms to manage their money, make investments, and store sensitive data. With the help of advanced technologies, fintech companies are now able to offer greater visibility into transactions, data usage, decision-making processes, and compliance. Technology-driven transparency not only enhances user confidence but also improves operational efficiency, accountability, and regulatory alignment.

1. Strengthening User Trust

Transparency about how data is collected, processed, and used helps build trust. Technologies such as automated consent logs, real-time privacy dashboards, and blockchain-based audit trails empower users to see exactly what happens with their information. This reduces uncertainty and fosters confidence, especially in first-time or cautious fintech users.

2. Enhancing Regulatory Compliance

Fintech firms must comply with strict data protection and financial regulations. Technologies such as RegTech tools and AI-based compliance monitoring ensure that companies stay aligned with legal frameworks like GDPR, India's DPDP Act, and RBI guidelines. Automated reporting and audit features also help organizations respond quickly to regulatory audits and avoid penalties.

3. Improving Customer Service and Communication

Transparent fintech apps provide users with real-time notifications, detailed transaction histories, and clear breakdowns of fees and charges. This enhances the user experience and reduces support queries or disputes. Chatbots, interactive dashboards, and push alerts ensure users are never in the dark about their financial activity.

4. Reducing Fraud and Misuse

Technologies such as AI-based transaction monitoring, machine learning algorithms, and biometric verification help in proactively identifying suspicious behavior. When users are informed of any unauthorized access attempts or policy changes in real-time, they are more likely to trust the platform's integrity and take protective actions.

5. Empowering Users with Control

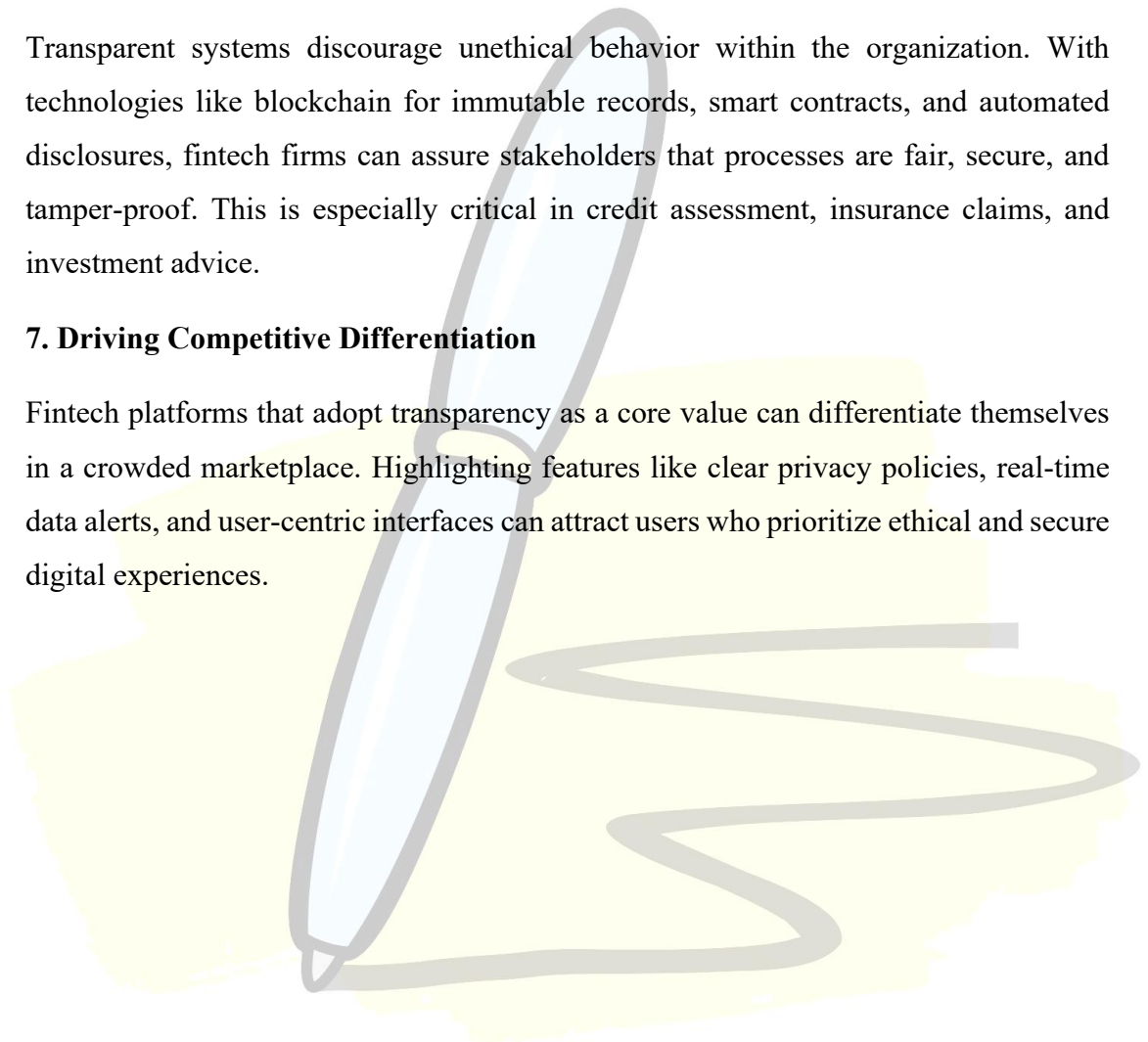
Transparency tools allow users to control their data preferences, permissions, and visibility settings. Features like "download my data" options, app permission management, and activity logs ensure that users can actively manage their digital financial footprint. This sense of control increases satisfaction and reduces fear of exploitation.

6. Encouraging Ethical Business Practices

Transparent systems discourage unethical behavior within the organization. With technologies like blockchain for immutable records, smart contracts, and automated disclosures, fintech firms can assure stakeholders that processes are fair, secure, and tamper-proof. This is especially critical in credit assessment, insurance claims, and investment advice.

7. Driving Competitive Differentiation

Fintech platforms that adopt transparency as a core value can differentiate themselves in a crowded marketplace. Highlighting features like clear privacy policies, real-time data alerts, and user-centric interfaces can attract users who prioritize ethical and secure digital experiences.



1.3. Company Profile:



1.3.1. History and Background of PB Fintech Limited

PB Fintech Limited is a leading Indian financial technology company headquartered in Gurugram, Haryana. Established in 2008, the company operates prominent digital platforms—Policybazaar and Paisabazaar—that have revolutionized the way consumers in India access insurance and lending products.

Flagship Platforms

- **Policybazaar:** Launched in 2008, Policybazaar is India's largest online insurance aggregator. It offers a wide range of insurance products, including health, term, motor, and travel insurance, allowing users to compare and purchase policies from various insurers. The platform aims to increase transparency and awareness among Indian households about the financial impact of unforeseen events like death, disease, and damage.
- **Paisabazaar:** Introduced in 2014, Paisabazaar is a digital marketplace for personal credit products. It enables consumers to compare and apply for various financial products such as personal loans, credit cards, and loans against property. The platform serves a diverse customer base across different credit profiles and income levels.

Business Model and Operations

PB Fintech operates through two main segments:

- **Insurance Services:** This segment includes insurance broker services provided through Policybazaar, facilitating the purchase of insurance products online.
- **Other Services:** This encompasses online marketing, consulting, and support services, primarily offered through Paisabazaar, catering to the financial services industry.

The company's platforms leverage proprietary technology and data analytics to provide user-friendly experiences, enabling consumers to make informed financial decisions.

Financial Highlights

As of the fiscal year ending March 2024, PB Fintech reported consolidated revenues of ₹34.38 billion. The company has a workforce of over 14,000 employees, supporting its operations across India and internationally.

Leadership

PB Fintech was co-founded by Yashish Dahiya, who serves as the Executive Chairman and CEO. Other key executives include Alok Bansal, Co-Founder and Executive Vice Chairman, and Sarbvir Singh, Executive Director and Joint Group CEO.

Through its innovative platforms, PB Fintech continues to play a pivotal role in enhancing financial inclusion and literacy in India, making insurance and credit products more accessible to the masses.



PB Fintech Limited, the parent company of Policybazaar and Paisabazaar, is a prominent Indian financial technology firm headquartered in Gurugram, Haryana. Since its inception in 2008, the company has been at the forefront of revolutionizing the insurance and lending sectors in India through its digital platforms.

1.3.2. Mission

PB Fintech's mission is to simplify the lives of consumers by providing easy access to financial services. The company is committed to leveraging technology and innovation to enhance financial literacy and empower customers in making informed decisions. A key aspect of their mission involves promoting transparency in the insurance and lending sectors, aiming to bridge the information gap faced by consumers. By offering platforms where users can compare various insurance policies and financial products, PB Fintech intends to demystify the financial decision-making process.

1.3.3. Vision

PB Fintech envisions a future where every Indian household is financially secure and well-informed about the financial implications of life's uncertainties. The company aims to be a catalyst in increasing transparency for consumers and facilitating online, research-based purchases of insurance and lending products. Through its consumer-centric approach, PB Fintech seeks to empower individuals to make informed financial choices.

1.3.4. Core Values

- **Customer-Centricity:** Prioritizing the needs and well-being of customers by providing transparent, accessible, and user-friendly financial solutions.
- **Innovation and Technology:** Harnessing cutting-edge technology and data analytics to develop innovative financial products and services that cater to diverse consumer needs.
- **Transparency and Integrity:** Maintaining honesty and openness in all dealings, ensuring that customers have clear and accurate information to make informed decisions.
- **Inclusivity and Accessibility:** Striving to extend financial services to underserved and underprivileged segments of society, promoting inclusive growth and equitable development.
- **Environmental and Social Responsibility:** Committing to sustainable practices that respect and protect the environment, and engaging in corporate social responsibility initiatives that contribute positively to society.

1.3.5. SWOT Analysis of PB Fintech Limited

Strengths

- **Strong Brand Portfolio:** Policybazaar and Paisabazaar are leading platforms in the Indian fintech space, with high brand recall and trust.
- **First-Mover Advantage:** Among the earliest players to digitize insurance aggregation and financial product comparison in India.
- **Large Customer Base:** Serves millions of users with high customer engagement, creating strong data-driven capabilities.
- **Technology-Driven Operations:** Advanced analytics and AI-backed recommendation engines enhance personalization and customer experience.
- **Strategic Partnerships:** Collaborates with a wide range of insurance companies and financial institutions, expanding its product offerings.

Weaknesses

- **Heavy Dependence on Online Model:** While this enables scalability, it also limits access in rural or less digitally literate markets.
- **High Marketing and Operational Costs:** Significant spending on customer acquisition and brand promotion affects profitability.
- **Limited Global Presence:** Operations are largely concentrated in India, with minimal international footprint compared to global fintech peers.

Opportunities

- **Growth in Digital Insurance and Lending:** Rising digital adoption in India and increased awareness of financial planning support long-term demand.
- **Untapped Rural and Tier-2/3 Markets:** Huge scope to expand reach through vernacular interfaces and offline-to-online strategies.
- **Cross-Selling Potential:** Large customer database offers room to upsell or cross-sell new financial products like investments or advisory services.
- **Expansion into Embedded Finance:** Can integrate fintech solutions into third-party platforms to diversify revenue streams.

Threats

- **Intense Competition:** Faces strong competition from other digital platforms like BankBazaar, Coverfox, and fintech startups.
- **Regulatory Risks:** Changes in insurance or financial sector regulations (IRDAI, RBI) can impact business operations.
- **Cybersecurity Threats:** Being a digital-first company, any breach of customer data could severely damage its reputation and trust.
- **Economic Slowdowns:** Consumer spending on insurance and credit may decline during periods of economic uncertainty or inflation.

1.4. Statement of the Problem:

With the rapid growth of fintech applications, users are increasingly reliant on digital platforms for financial transactions, investment management, and personal banking. While these applications offer convenience and innovation, they also raise significant concerns about data privacy and security. Users often share sensitive personal and financial information on these platforms, making them vulnerable to data breaches, unauthorized access, and misuse of information. Despite regulatory efforts and the implementation of security features by fintech firms, there remains a gap in understanding how users perceive these efforts and whether they trust the platforms they use. This study seeks to investigate the perceptions, concerns, and trust levels of users regarding data privacy and security in fintech applications, and to identify the key factors influencing these perceptions.

1.5. Objective of the Study:

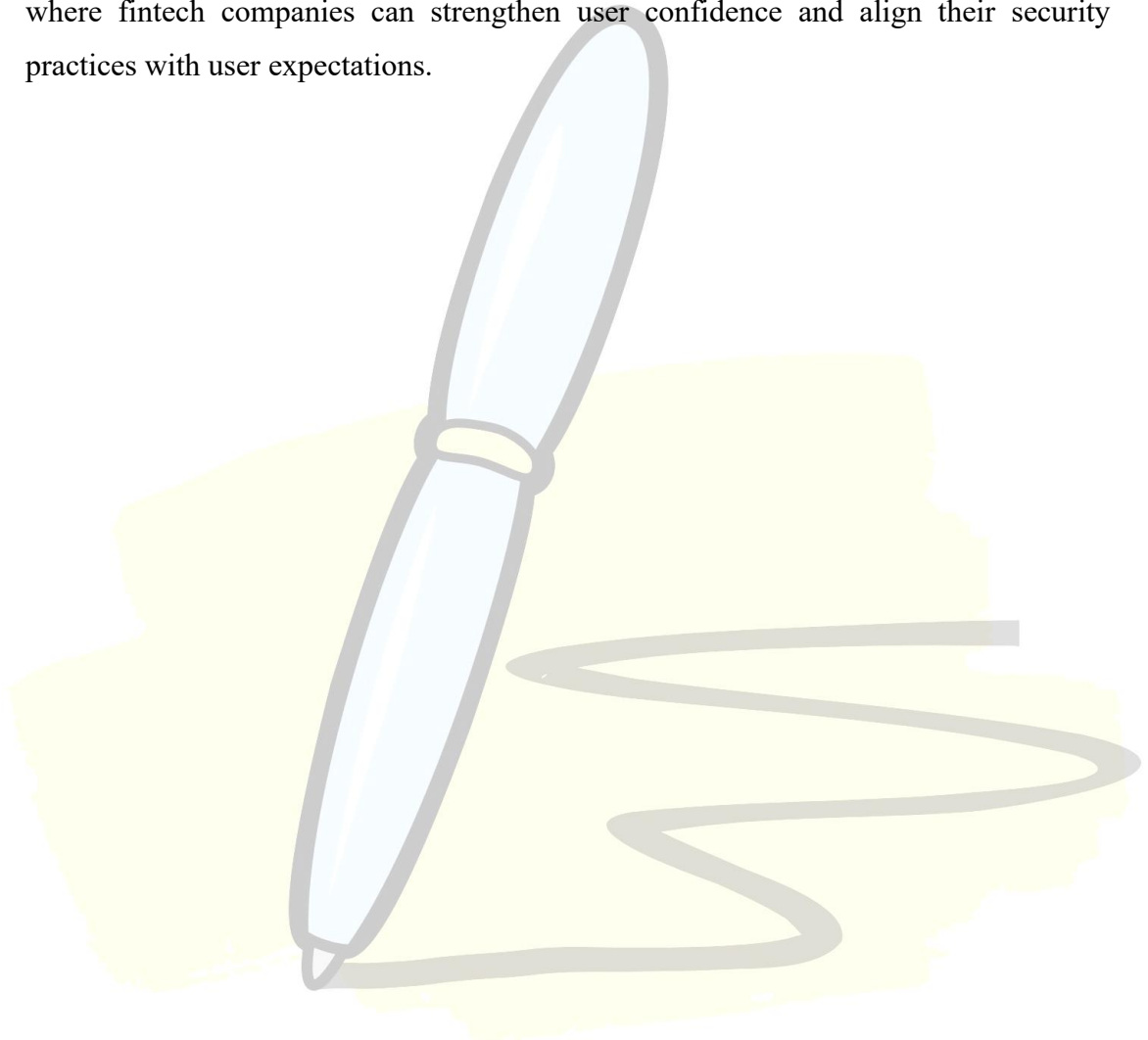
1. To analyse user perception of the safety features implemented by fintech platforms.
2. To identify key concerns among users regarding data breaches and misuse of personal information.
3. To explore the influence of privacy policies and app permissions on user confidence.
4. To understand user behavior related to sharing personal and financial data on fintech platforms.

1.6. Scope of the Study:

The study focuses on understanding user perceptions of data privacy and security in fintech applications. It is limited to users of fintech platforms and is based on responses collected through a structured questionnaire from a sample of 100 participants. The study provides insights into user concerns, trust levels, and behavior related to data security features in fintech services.

1.7. Purpose of the Study:

The purpose of this study is to gain a deeper understanding of how users perceive data privacy and security in fintech applications. As digital financial services become increasingly integral to everyday transactions, it is essential to assess whether users feel their personal and financial information is adequately protected. This study aims to explore user awareness, trust levels, and concerns regarding data handling practices in fintech platforms. By examining these perceptions, the study seeks to highlight areas where fintech companies can strengthen user confidence and align their security practices with user expectations.



CHAPTER 2

LITERATURE REVIEW

1. Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). “Data Security, Customer Trust and Intention for Adoption of Fintech Services: An Empirical Analysis from Commercial Bank Users in Pakistan.”

The DAS, PEU, PU, CT, and FP had been found to affect the intention to use fintech service in Pakistan. The study then utilizing data from 297 attended respondents and assesses the data by Partial Least Squares Structural Equation Modeling (PLS-SEM) confirms that DAS, PEU, PU, FP and CT all significantly influence adoption intentions. In addition, PEU and DAS are significant in predicting CT and FP whereas promotion has virtually no effect on trust. The Technology Acceptance Model (TAM) literature is extended and it is demonstrated that, for fintech technology, strong data protection and customer trust are essential to enhance adoption of fintech technology in emerging economies.

2. Nangin, M. A., Barus, I. R. G., & Wahyoedi, S. (2020). “The Effects of Perceived Ease of Use, Security, and Promotion on Trust and Its Implications on Fintech Adoption.”

In this paper, we evaluate PEOU, security, and promotion’s effect on trust and fintech adoption in Indonesia, using Sakuku users. A SEM-PLS analysis of the data collected from 100 respondents shows that PEOU and promotion predict trust, while security does not. The study also shows that trust is the key to fintech adoption and additionally recommends that fintech brands improve user experience and promotional efforts, if they want to increase usage, especially of young, digitally literate consumers.

3. Nayak, K., Singh, P., & Dave, P. (2021). “Does Data Security and Trust Affect the Users of Fintech?”

Using German fintech users as a context, this study investigates how customer trust, data security, value-added features, user interface, and fintech promotion shape the intention for adopting fintech services. The study finds using SPSS and AMOS with 209 valid responses that data security, trust and promotion are found in descending order to have a significant effect to fintech adoption. However, the study outlines the need for creating sound cybersecurity frameworks and integrity building techniques in order to enhance fintech acceptance and abate digital crime threats.

4. Dash, B., Sharma, P., & Ali, A. (2022). “Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech.”

I discuss the current discussions about utilizing federated learning as a privacy-preserving method of analyzing personal identifiable data (PII) in fintech in this conceptual review. Federated learning, a decentralized data processing model that improves data privacy by keeping the user data local to device, is explored by this paper. We then review various applications of this approach in fintech, in particular around complying with data protection regulations, such as GDPR. This work describes how data minimization and anonymization yield privacy benefits as well as federated learning enabled principles, and its associated challenges such as privacy leak and scalability.

5. Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). “Encryption Techniques for Financial Data Security in Fintech Applications.”

In this paper, the encryption techniques, which act as encryption method for protecting the financial data among the fintech, are presented together with symmetric, asymmetric, hybrid and homomorphic encryption. It highlights the protection mobile banking and digital payments gain from end-to-end encryption. This work reviews strengths, limitations, and practical applicability of each technique, and further,

discusses some future trends such as post quantum cryptography and AI based adaptive security. Evolving encryption strategies are essential to both secure fintech innovation and regulatory compliance in an ever more digital financial landscape, the authors stress.

6. Abdul-Rahim, R., Bohari, S. A., Aman, A., & Awang, Z. (2022). “Benefit–Risk Perceptions of FinTech Adoption for Sustainability from Bank Consumers’ Perspective: The Moderating Role of Fear of COVID-19.”

This study explores perceived benefits and risks of fintech services, how COVID-19 fear moderates these perceptions, and the impact of fintech adoption on sustainability. The data (N=400) collected from Malaysian bank consumers were used in structuring a structural equation modeling (SEM) approach where perceived benefits were shown to significantly influence adoption, while perceived risks do not. This article shows that fear of COVID-19 moderates the benefit adoption relationship and mediates the risk adoption relationship. The results suggest that using consumer sentiment and limiting perceived risk can encourage the placement of fintech services favorable, improving economic and environmental results.

7. Yu, A.-P., Xu, C., & Cho, S.-E. (2024). “Factors Affecting Customer Use Intention of MyData Services in the Fintech Industry.”

This study examines how MyData service attributes (i.e., transparency, security, controllability, diversity, and personalization) influence perceived value and the customer's intention to use MyData services in the Korean fintech sector. Regression techniques are applied and analyzed on a survey of 291 participants. Results reveal that transparency, security, and personalization have direct impact on user intention and that perceived value mediates most of these relationships. The results contribute to knowledge regarding how user centric design and strong security can improve customer's engagement with personal data management in fintech and how service innovation and trust capacity can be built on such foundations.

8. Nguyen, D. D., Nguyen, T. D., Nguyen, T. D., & Nguyen, H. V. (2021). “Impacts of Perceived Security and Knowledge on Continuous Intention to Use Mobile Fintech Payment Services: An Empirical Study in Vietnam.”

Using mobile fintech services, this empirical study addresses how perceived security, knowledge, and post-adoption satisfaction affect users’ intention to continue using mobile fintech services in the context of Vietnam. Using data from 352 users, the study applies the Extended Post Acceptance Model (EPAM) to test the impact of security and knowledge on confirmation and perceived usefulness, which influence satisfaction and attitude. Nevertheless, continued usage is not a function of security. The results highlight the need for fintech companies to increase users’ knowledge and build their digital trust to avoid fostering low engagement in a context of emerging economies.

9. Dorfleitner, G., & Hornuf, L. (2019). “FinTech and Data Privacy in Germany: An Empirical Analysis with Policy Recommendations.”

In this book, an empirical survey was undertaken into how over 500 German fintech employ data protection – specifically with regard to GDPR regulations. In a systematic analysis of privacy policies in different fintech segments, the authors find that firms in all fintech space recognize privacy as important, though varying substantially in how they achieve privacy and how transparently they communicate their efforts. The legal adherence gaps are identified, and need for the standardized regulation is highlighted. The result contributes to the discussion on reconciling innovation and data protection in fintech, providing actionable policy recommendations to regulators and practitioners in the context of the European digital finance landscape.

10. Aldboush, H. H. H., & Ferdous, M. (2023). “Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust.”

In light of the ethics and privacy challenges further empowered by big data and AI applications developed in fintech, this systematic literature review examines the ethical and privacy challenges in fintech, the risks resulting from data use in fintech, and the

proposed legal and regulatory frameworks to oversee privacy in fintech. It draws on 39 peer-reviewed studies to focus on central questions about transparency, ownership and data control, clarifies bias, and underscores how central corporate digital responsibility (CDR) is for a free internet as companies compete to reshape citizens' lives and their intimacies. However, the study offers best practices such as encryption, transparency in the use of data, and employee training. Finally, it suggests that market leaders can foster ethical cultures and CDR practice and benefit from increased customer trust and competitive advantage; the more competent CDR practice, the higher the level of compliance with privacy laws; discussions on innovation, data, and ethics are siloes; while trust is the essence of success with a fintech brand, which is the essence of sustainable fintech success.

11. Ahmad Juma'h, Yazan Alnsour, & Hasan Kartal (2025). "Perceived Security and Privacy in Cryptocurrency Apps: A Text Mining and Ordinal Regression Approach."

In this study we examine how perceived security and perceived privacy affect user satisfaction and ratings on applications related to cryptocurrency. Using text mining and ordinal regression analysis of over 64,000 user reviews from 140 Android based cryptocurrency apps, researchers found that the apps with greater perceived security received better reviews. Based on Protection Motivation Theory, the study finds that although these apps outperform productivity apps, they are still behind on mainstream fintech and banking apps. The findings indicate that improved app success results from trust in privacy and data protection on the users' part. This study provides a complete framework through which app developers and app marketers can improve user satisfaction with more secure software.

12. Indra Dharma Wijaya, Endang Siti Astuti, Edy Yulianto, & Yusri Abdillah (2025). “Examining the Impact of Perceived Usefulness on Micro-Entrepreneurs' Intentions to Use Fintech Peer-to-Peer Lending Applications with Perceived Security as a Mediating Factor.”

The relationship with perceived usefulness, perceived security, and intention for Indonesian micro entrepreneurs to use fintech P2P lending apps is the focus of this research. Also using data from 204 respondents collected through quantitative explanatory design and PLS-SEM, the results indicate that perceived usefulness functions positively with perceived security and user intention. This relationship is also mediated by perceived security. Open innovation is presented as a tool for mitigating trust problems involved in entering customers' sensitive data and solve regulatory issues – providing potential fintech developers and policymakers with a way to speed up adoption rates. Examining underrepresented micro-entrepreneur market populations, it adds to financial inclusion literature.

13. Taewoo Roh, Young Soo Yang, Shufeng Xiao, & Byung Il Park (2022). “What Makes Consumers Trust and Adopt Fintech? An Empirical Investigation in China.”

As an empirical study, this dissertation combines Information Systems Success Model and Theory of Reasoned Action to investigate the effect of trust on the adoption of fintech services in China. Based on survey data, this study identifies system, information, and service quality as basic factors affecting user trust. In the other hand, trust has a big effect on consumer attitudes, and intention to adopt fintech. However, the results show that privacy and security matter a lot when it comes to influencing trust, a development that fintech managers should build user centric platforms that help address behavioral uncertainty. The fintech adoption literature is supplemented with this study by providing a context in which to view the behavior of consumers that are situated within a high adoption economy.

14. David Laurent & Robin Sinz (2019). “FinTech: The Role of Perceived Cybersecurity and Organizational Trust—Investigating from a Customer Perspective in Sweden.”

The objective of this master’s thesis is to examine how perceived cybersecurity and organizational trust drive the consumer adoption of mobile payment fintech applications. Using the Technology Acceptance Model (TAM) and employing the quantitative methods utilizing logistic and multiple regression analyses, this study examines the predictors of adoption across multiple domains and finds perceived usefulness, device security, ergonomics, and trust as significant predictors. The research shows how security threats threaten user comfort with 'always available' digital platforms and demonstrates the dual requirement of availability and safety in an overwhelmingly optimistic system. The results underscore the importance of trust construction through rigorous security design in achieving the growth of fintech and demonstrate managerial implications for building user trust and technological acceptance.

15. Jen Sheng Wang (2021). “Exploring Biometric Identification in FinTech Applications Based on the Modified TAM.”

In this study we adapt the Technology Acceptance Model (TAM) to examine its ability to account for the acceptance of biometric identification through the addition of perceived trust and privacy into the model in applications of fintech. The study uses scenario methods and analytic hierarchy process (AHP) methods to evaluate user preferences of biometric method such as facial and voice recognition. Biometrics provide an improvement on security, but are heavily dependent on what users perceive as their privacy and trust. We are able to successfully predict technology adoption using the modified TAM framework and also demonstrate a need for fintech services to overcome biometrics related issues. The work provides a strategic roadmap on the need to optimize security against user comfort in identity verification systems.

16. Hassan AbdulRedha AlHassan, Avraam Papastathopoulos, & Haitham Nobanee (2025) “Measuring Perceived Security in FinTech Services: Developing a Dynamic Scale.”

In response, this study attempts to fill this gap of a measurement instrument for perceived security in FinTech services. The authors then developed the FinTech Security Adoption Scale (FT-SAS), using a five-stage scale development process using bifactor exploratory structural equation modeling (ESEM) and data from 1,377 users aged 18 and older in the U.S. and U.K. The study identifies five core dimensions of perceived security and demonstrates that a user's perception of FinTech security is along a multidimensional continuum. By bridging this gap between technology adoption models and FinTech specific security concerns, the results provide both theoretical and practical insights to user behavior across mature markets.

17. Johan Ariff Jafri, Syajarul Imna Mohd Amin, Aisyah Abdul Rahman, & Shifa Mohd Nor (2024) “A Systematic Literature Review of the Role of Trust and Security on FinTech Adoption in Banking.”

In this systematic literature review, I analyze 26 studies from the Scopus and Web of Science databases from 2009 to 2022 to capture how trust and security motivate the adoption of a FinTech platform in the banking sector. Using thematic analysis and ROSES framework, the authors found that most of the predictors are performance expectancy, trust and perceived security. By using the TCCM (Theory, Context, Constructs, Method) framework, this thesis illustrated significant research gaps and future agendas. This study points out the urgency of merging multiple theories to cover all the aspects of modeling FinTech behavioral intention, and provides the advice to governors and FinTech companies towards strengthening secure adoption and building consumer trust.

18. Yoonyoung Hwang, Sangwook Park, & Nina Shin (2021) “Sustainable Development of a Mobile Payment Security Environment Using FinTech Solutions.”

Drawing on the issues relating to security in mobile commerce, this study investigates how platform and technology security affect perceptions of mobile payment services (MPS). In this paper, the authors develop a model to assess the role of platform (subjective) and technology (objective) security in influencing MPS success determinants (i.e., trust, convenience, and interoperability) using data from a survey of 356 South Korean MPS users. The research observed that user belief of security has a significant impact upon their satisfaction and ongoing intention of usage. The results offer design recommendations for MPS providers to differentiate between user perceived and technical security aspects, leading to more trust and long-lasting integration of digital financial services.

19. Muhammad Ali, Syed Ali Raza, Bilal Khamis, Chin-Hong Puah, & Hanudin Amin (2021) “How Perceived Risk, Benefit, and Trust Determine User FinTech Adoption: A New Dimension for Islamic Finance.”

This paper explores the FinTech adoption of FinTech products and services, and uses Islamic finance as a base, in which a users’ perceived risk, benefits and trust are used as variables in determination D. Using a structured survey and structural equation modeling, the study empirically validated that while there is a positive relationship between trust and perceived benefits and subsequent adoption, the perceived risk negatively affected user intention. Paper argues for Sharia compliant FinTech offering and brings out the cultural and philosophical underpinnings of financial decision making. The study contributes to the FinTech literature by customizing analysis for Islamic financial contexts and proposing user centric concepts of building FinTech trustworthiness and decreasing related risk concerns.

20. Gregor Dorfleitner, Lars Hornuf, & Julia Kreppmeier (2023) “Promise Not Fulfilled: FinTech, Data Privacy, and the GDPR.”

This thesis deals with how the General Data Protection Regulation (GDPR) impacts the data privacy practices of 276 German FinTech companies. Using text analysis of privacy statements, the authors show a decline in readability as well as a rise in the use of standardized, more difficult to read language. The results show that by inadvertently becoming GDPR compliant, transparency and user comprehension could have been reduced. Moreover, while external investors and legal capital influenced privacy practices before GDPR, they did not influence after GDPR. The study then finds that GDPR is not effective to increase actual privacy awareness and further specify where regulatory improvements are needed.

21. Singh, S., Sahni, M. M., & Kovid, R. (2020) “What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model.”

In order to study FinTech adoption, this study extends the traditional Technology Acceptance Model (TAM) by including constructs from UTAUT, ServPerf, and WebQual 4.0. Then, in a structural equation modeling analysis of 439 responses to a survey of internet users, the authors find that perceived usefulness and social influence are key determinants of behavioral intention, and that ease of use and social influence directly affect actual use. The results provide practical guidelines for FinTech service providers regarding how to increase user engagement and promote security, responsiveness and ease of use.

22. Bouteraa, M., Chekima, B., Lajuni, N., & Anwar, A. (2023) “Understanding Consumers’ Barriers to Using FinTech Services in the United Arab Emirates: Mixed-Methods Research Approach.”

To identify barriers to FinTech adoption in the UAE, this study undertakes an exploratory sequential mixed methods approach. We conducted initial interviews with banking professionals, to identify six key initial barriers to introducing Islamic finance in high income Western countries that were later tested with a survey of 332 bank

customers. As expected, individual, technology, organizational, and environmental factors were all found to affect consumers' intention to use FinTech. In addition, the study extends the UTAUT model by including these new variables and demonstrates that the UTAUT model is applicable in a Middle Eastern context.

23. Vasquez, O., & San-Jose, L. (2022) "Ethics in FinTech Through Users' Confidence: Determinants That Affect Trust."

The ethical dimensions of trust in FinTech platforms are investigated in this research by analysing six key determinants of trust: risk, reputation, regulation, inclusion, price and website information quality. By carrying out content analysis of FinTech company websites (n=45) and Delphi method comprised of 11 experts, the research results revealed all factors impacted trust, however risk (security, privacy, financial) was universally agreed to be the determining factor that would determine user trust of FinTech services. The research shows that good, ethical FinTech behavior is led by trust, with users' confidence riding on transparent, inclusive, and secure business models. In addition, it extends the Technology Acceptance Model by considering trust and ethics as essential elements in the adoption of technology.

24. Alwi, S., Alpandi, R. M., Salleh, M. N. M., Basir, I. N., & Md Ariff, F. F. (2019) "An Empirical Study on the Customers' Satisfaction on FinTech Mobile Payment Services in Malaysia."

Using theories of dissonance, assimilation, and contrast, this quantitative study explores factors which influence customer satisfaction with FinTech mobile payment services in Malaysia. Data gathered from users were from a structured questionnaire, and using Pearson correlation analysis, it was found that security and privacy are the strongest predictor of satisfaction, and followed by service quality, information presentation, and ease of use. The finding indicates that financial institutions have to focus on communicating clearly to and protecting the digital assets of customers diligently to enforce loyalty and customer satisfaction in the competitive FinTech world.

25. Osman, Z., & Ing, P. (2021) “Does Security Concern, Perceived Enjoyment and Government Support Affect Fintech Adoption? Focused on Bank Users.”

FinTech adoption among Malaysian bank users is studied through this research with use of Technology Acceptance Model (TAM). The analysis is conducted based on the result of 500 survey responses and shows that security concerns and government support positively affect the users' adoption intention of FinTech services, while perceived enjoyment doesn't. Across all variables, the moderating role of age was insignificant. The findings highlight the need to prioritize data security and institutional support, as well as show that safety and regulatory assurance becomes a key component in building trust, and ultimately, adoption of digital financial services.

26. Alalwan, A. A., Baabdullah, A. M., Al-Debei, M. M., Raman, R., Alhitmi, H. K., Abu-ElSamen, A. A., & Dwivedi, Y. K. (2023). “Fintech and contactless payment: Help or hindrance? The role of invasion of privacy and information disclosure.”

This study examines how the personalization privacy paradox influences continued intention (CIN) to use contactless payment in Saudi Arabia. Using survey data from 297 users, the researchers used structural equation modeling to confirm that perceived privacy invasion and information disclosure value lead to CIN. In the study, the protection motivation theory is combined with the personalization–privacy paradox in one model. In this thesis we find that while personalization fosters user interest, privacy worries prevent adoption. As such, FinTech developers must balance personalization with privacy.

27. Chan, R., Troshani, I., Hill, S. R., & Hoffmann, A. (2022). “Towards an understanding of consumers' FinTech adoption: The case of Open Banking.”

To assess adoption by consumers of Open Banking, the authors adopt the Unified Theory of Acceptance and Use of Technology (UTAUT) to extend the model to include perceived risk, initial trust and financial literacy. An analysis of 456 Australian survey responses using partial least squares structural equation modeling indicated

performance expectancy, effort expectancy and social influence significantly predicts usage intention. More specifically, interestingly, initial trust can diminish the negative effect of perceived risk. Practical implications to policy makers and FinTech providers in enhancing adoption through trust building strategies are presented by the study.

28. Al Nawayseh, M. K. (2020). “FinTech in COVID-19 and Beyond: What Factors Are Affecting Customers’ Choice of FinTech Applications?”

In this case, we focus on the Jordanian context during the COVID 19 crisis and adopt SEM-PLS to understand the impact of trust, perceived benefits and social norms on FinTech adoption. In using a sample of 500 potential FinTech application users, the research found that perceived benefits and social influence positively influenced intention to use FinTech applications and perceived technology risks had no significant impact. In mediating trust was a major mediator. However, the study highlights, FinTechs are part of ensuring financial resilience and inclusion during the ‘crisis’, particularly in developing countries.

29. Juma’h, A., Alnsour, Y., & Kartal, H. (2025). “The impact of security and privacy perceptions on cryptocurrency app evaluations by users: A text mining study.”

Using sentiment analysis and ordinal regression on over 64,000 user reviews from the Google Play store, this study uses privacy and security perceptions to explore how these perceptions influence cryptocurrency app ratings. We demonstrate that while better security features result in higher ratings, privacy and security threats lead to lower user evaluations. The model proves that user trust is the core on satisfaction with a pseudo- R^2 of 0.25. To the FinTech literature, the study contributes by using Protection Motivation Theory to app adoption behavior in the cryptocurrency domain.

30. Gai, K., Qiu, M., & Sun, X. (2018). “A survey on FinTech.”

In this comprehensive survey, we reexamine the literature and classify FinTech under five technical dimensions: security and privacy, data techniques, hardware and infrastructure, applications and management, and service models. The study also argues the complexity of FinTech implementation is growing, cybersecurity is important, and integrated data relies solutions is on the rise. The theoretical FinTech framework is proposed and issues of outsourcing, cloud infrastructure, and privacy protection are underlined. The paper is a great resource for those who wish to learn what the current FinTech landscape of now and where future research directions are headed.

31. Li, C., Khaliq, N., Chinove, L., Khaliq, U., & Oláh, J. (2023). “Consumers’ Perception of Risk Facets Associated with Fintech Use: Evidence from Pakistan”.

This study investigates the impact of eight perceived risk dimensions (performance, financial, social, time, security, legal, psychological, and overall risk) on consumers’ intention to adopt fintech in Pakistan using structural equation modeling (SEM) on data from 210 respondents. The results highlight that performance risk, financial risk, and overall risk significantly and negatively affect adoption intentions, while the remaining factors showed no significant effect. The research emphasizes the necessity for fintech service providers to minimize operational risks and build trust to encourage greater adoption, especially in emerging markets like Pakistan.

32. Meyliana, Fernando, E., & Surjandy. (2019). “The Influence of Perceived Risk and Trust in Adoption of FinTech Services in Indonesia”.

Using the Technology Acceptance Model (TAM) as the theoretical foundation, this quantitative study explored how trust and perceived risk affect the adoption of fintech services in Indonesia. Based on 548 survey responses analyzed via Smart PLS SEM, the research found that trust significantly influences perceived usefulness, while perceived risk had no direct impact on users' attitudes or adoption behavior. The study contributes to understanding the psychological determinants of fintech usage and emphasizes the role of trust over risk in user acceptance.

33. Appiah, T., & (2025). “The Interplay of Perceived Benefit, Perceived Risk, and Trust in Fintech Adoption: Insights from Sub-Saharan Africa”.

This study applies both PLS-SEM and fuzzy-set qualitative comparative analysis (FSQCA) on data from four Sub-Saharan African countries to assess how benefit and risk factors affect fintech adoption. The findings show that performance expectancy, economic benefits, and effort expectancy promote adoption, while legal, security, and privacy risks inhibit it. Trust was found to mediate the negative effects of perceived risk. This research enriches the UTAUT model and offers a nuanced perspective on the factors influencing fintech uptake in developing economies.

34. Nigam, A., Khan, F. S., Mazhar, S. S., Chaudhary, N., Haque, E., Mir, M. A., & Ansari, M. S. (2024). “Consumer Perceptions and Attitudes Towards E-Payment Services Offered by Fintech Companies: Evidence from India”.

This paper examines Indian consumers’ attitudes toward e-payment fintech services using SEM through AMOS with 420 valid responses. The study identified trust, convenience, technological familiarity, and security as key factors shaping consumer perceptions and acceptance. The research contributes to fintech literature by offering actionable insights for service providers to optimize user engagement and enhance satisfaction through targeted design and marketing strategies.

35. Meng, W., Zhu, L., Li, W., Han, J., & Li, Y. (2019). “Enhancing the Security of FinTech Applications with Map-Based Graphical Password Authentication”.

Focusing on improving authentication in fintech applications, this study introduces RouteMap, a novel map-based graphical password scheme designed to combat issues with multiple password memory. The authors conducted comparative user studies involving 120 participants, including fintech professionals. Results demonstrated that RouteMap outperformed other schemes in both accuracy and memory retention, suggesting it as a promising alternative for secure and user-friendly fintech authentication systems.

36. Ryu, H.-S., & Ko, K. S. (2020). “Sustainable Development of Fintech: Focused on Uncertainty and Perceived Quality Issues”.

This study investigates how uncertainty and IT quality impact users’ continuance intentions in Fintech services. Using a trust-based model integrated with the Information Systems Success (ISS) model, the authors examined the effect of system, information, and service quality on perceived risk and trust. Data were collected from 218 Fintech users in South Korea. The findings showed that service quality significantly influences trust and mitigates uncertainty, which in turn improves the likelihood of continued use of Fintech. The study concluded that IT quality is crucial for Fintech sustainability and recommended practical design strategies for Fintech providers.

37. Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). “Data Privacy Laws and Their Impact on Financial Technology Companies: A Review”.

This review paper explores the implications of data privacy regulations on FinTech operations in the digital financial ecosystem. Utilizing a qualitative approach, the study synthesizes literature, legal frameworks, and policy documents. The authors highlight the "Innovation Trilemma" — the tension between innovation, consumer protection, and regulatory clarity. Findings emphasize the importance of ethical compliance, transparency, and adaptive regulation for FinTech growth. The paper concludes with a call for regulatory harmonization and ethical innovation to ensure sustainable and inclusive FinTech development.

38. Akmal, S., Talha, M., Faisal, S. M., Ahmad, M., & Khan, A. K. (2023). “Perceptions about FinTech: New Evidences from the Middle East”.

The study examines user perceptions of FinTech adoption and performance in the Middle East, using a cross-sectional survey conducted between November 2021 and February 2022. The researchers employed semi-structured questionnaires and SPSS for analysis. The findings suggest that digital banking is widely valued across demographics and significantly enhances financial institution performance. Cultural

attitudes, regulatory environments, and technological readiness influenced FinTech adoption in the region. The paper concludes that FinTech adoption is promising in the Middle East, particularly among younger, tech-savvy populations.

39. Aboalsamh, H. M., Khrais, L. T., & Albahussain, S. A. (2023). “Pioneering Perception of Green Fintech in Promoting Sustainable Digital Services Application within Smart Cities”.

This qualitative study explores how green FinTech can drive sustainability within smart cities, focusing on consumer perceptions and policy impact in Saudi Arabia. Interviews with participants and content analysis of six articles provided data. Results indicated that green FinTech encourages environmental investment and improves financial inclusion. However, regulatory limitations impede broader adoption. The study emphasizes that increasing public awareness and supportive policies are crucial for sustainable digital innovation and achieving national goals like Saudi Arabia’s Vision 2030.

40. Suryono, R. R., Budi, I., & Purwandari, B. (2021). “Detection of Fintech P2P Lending Issues in Indonesia”.

This research employs a qualitative case study approach, including Focus Group Discussions (FGDs) and online news analysis, to identify issues in Indonesia’s FinTech P2P lending sector. Using tools like VOS Viewer and NVIVO, the study categorizes challenges into themes such as data misuse, illegal platforms, and ethical marketing. Findings reveal widespread concern over data security and unregulated platforms despite rapid market growth. The study calls for stronger regulatory frameworks, public education, and ethical practices to ensure safe and sustainable P2P lending growth in Indonesia.

CHAPTER 3

RESEARCH METHODOLOGY

3.1. Research Design:

The research design adopted for this study is descriptive in nature. It aims to gain insights into user perceptions regarding data privacy and security in fintech applications. A mixed-method approach, combining both qualitative and quantitative techniques, has been employed to ensure a comprehensive understanding of the subject matter.

3.2. Sources of Data Collection:

3.2.1. Primary Data:

Primary data was collected through a structured questionnaire designed with Likert scale responses. The questionnaire focused on capturing user opinions and experiences related to privacy and data security features in fintech applications.

3.2.2. Secondary Data:

Secondary data was sourced from existing literature including academic journals, white papers, and online articles to support the primary findings and provide theoretical grounding for the study.

3.3. Sampling Design and Technique:

3.3.1. Sample Size:

The study was conducted with a sample size of 100 respondents.

3.3.2. Sample Unit:

The sample unit consists of individuals who actively use fintech applications for banking, payments, investments, or financial management.

3.3.3. Sampling Technique:

Convenient sampling technique was employed to select the respondents based on ease of access and willingness to participate.

3.4. Duration of the Study:

The duration of the study was 45 days.

3.5. Tools Used for Data Analysis:

The collected data was analyzed using percentage analysis, supported by tables and charts to present findings in a clear and concise manner.

3.6. Limitation of the Study:

- The study is limited to a sample size of 100 respondents, which may not represent the entire fintech user population.
- Data was collected using a convenient sampling method, which may introduce selection bias.
- Responses are based on self-reported perceptions, which may be influenced by personal experiences or lack of technical knowledge.
- The study is confined to a specific time frame of 45 days, limiting the scope of longitudinal analysis.
- Only commonly used fintech applications were considered, excluding enterprise-level or niche platforms.

CHAPTER 4

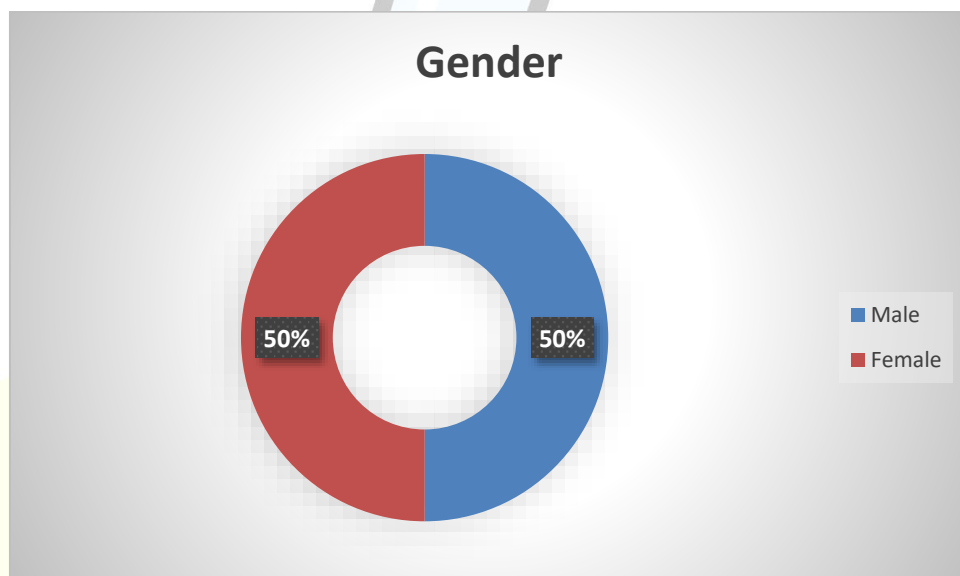
DATA ANALYSIS

1. Gender

Table no. 1

“Gender”	“No. of Respondents”	“Percentage”
“Male”	50	50%
“Female”	50	50%
“Total”	100	100%

Chart no. 1



Interpretation:

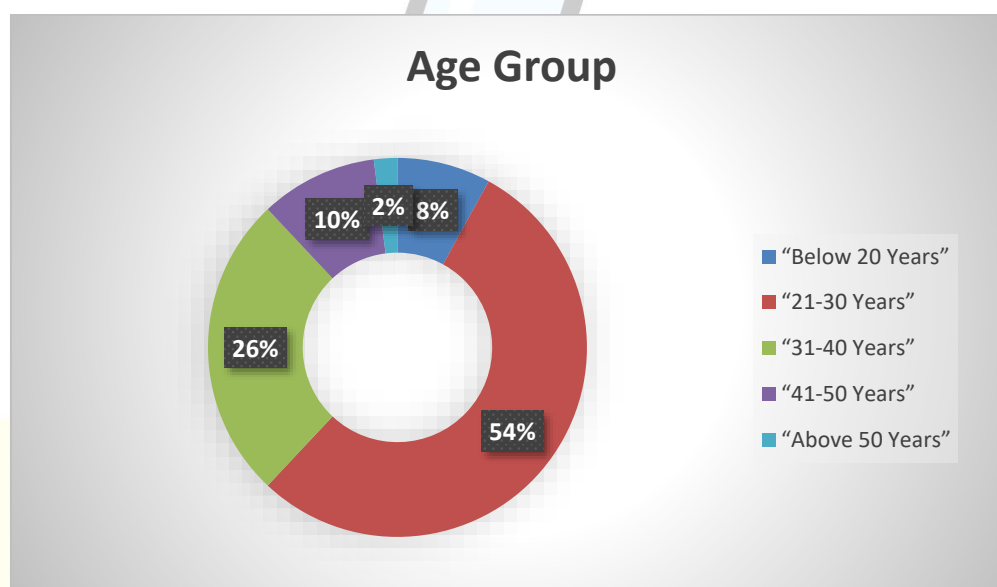
The gender distribution of respondents is evenly split, with 50% male and 50% female participants. This balanced representation ensures that the study reflects perceptions of data privacy and security in fintech applications across both genders.

2. Age Group:

Table no. 2

“Age Group”	“No. of Respondents”	“Percentage”
“Below 20 Years”	8	8%
“21-30 Years”	54	54%
“31-40 Years”	26	26%
“41-50 Years”	10	10%
“Above 50 Years”	2	2%
“Total”	100	100%

Chart no. 2



Interpretation:

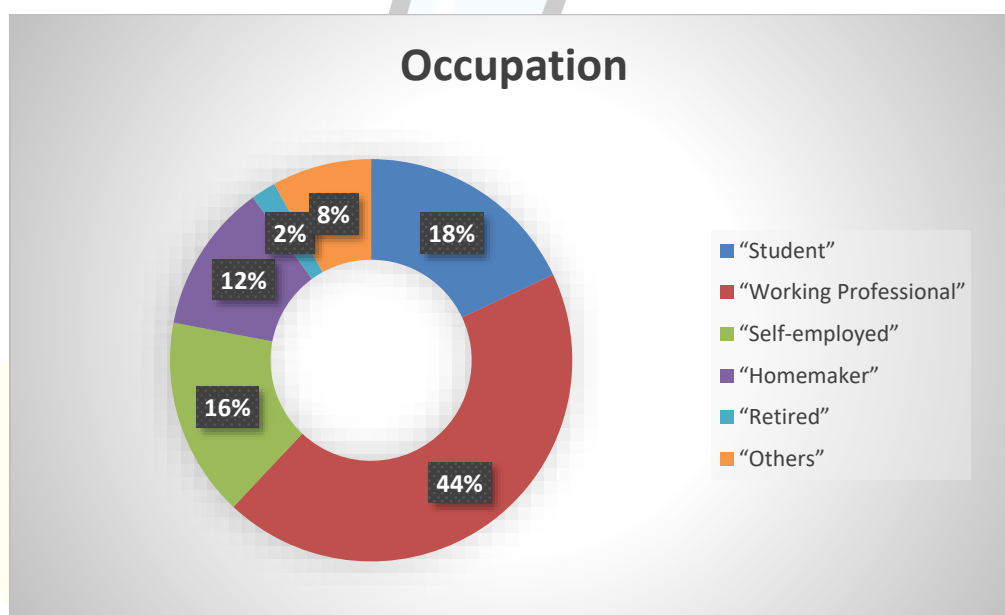
The majority of respondents (54%) belong to the 21–30 years age group, indicating that young adults are the most active users of fintech applications. This is followed by 26% in the 31–40 years group, showing that the user base is predominantly composed of tech-savvy and financially active individuals.

3. Occupation:

Table no. 3

“Occupation”	“No. of Respondents”	“Percentage”
“Student”	18	18%
“Working Professional”	44	44%
“Self-employed”	16	16%
“Homemaker”	12	12%
“Retired”	2	2%
“Others”	8	8%
“Total”	100	100%

Chart no. 3



Interpretation:

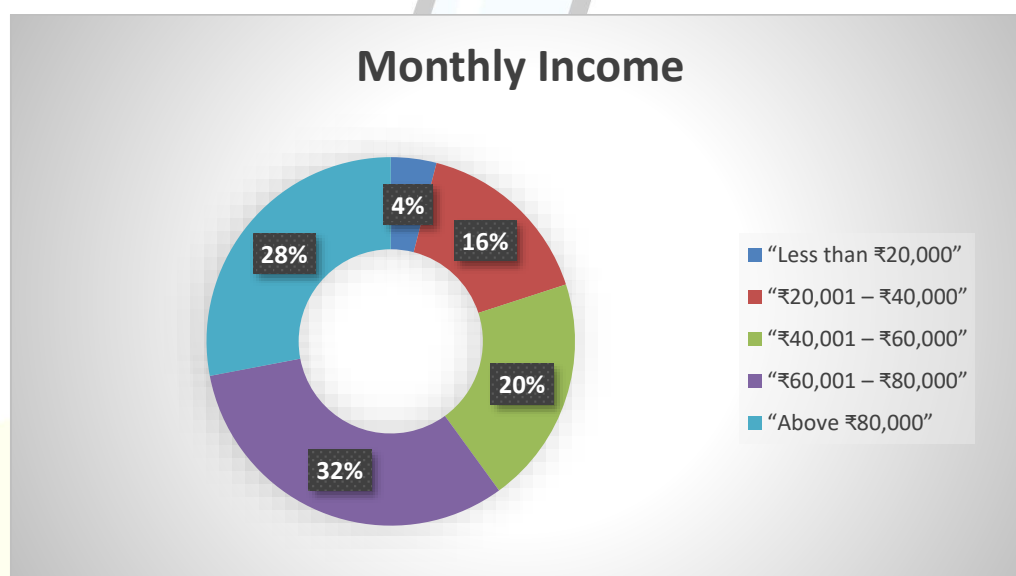
Most respondents (44%) are working professionals, suggesting that employed individuals are the primary users of fintech applications. Students (18%) and self-employed users (16%) also form significant user groups, indicating widespread adoption across various occupational segments.

4. Family Monthly Income:

Table no. 4

“Monthly Income”	“No. of Respondents”	“Percentage”
“Less than ₹20,000”	4	4%
“₹20,001 – ₹40,000”	16	16%
“₹40,001 – ₹60,000”	20	20%
“₹60,001 – ₹80,000”	32	32%
“Above ₹80,000”	28	28%
“Total”	100	100%

Chart no. 4



Interpretation:

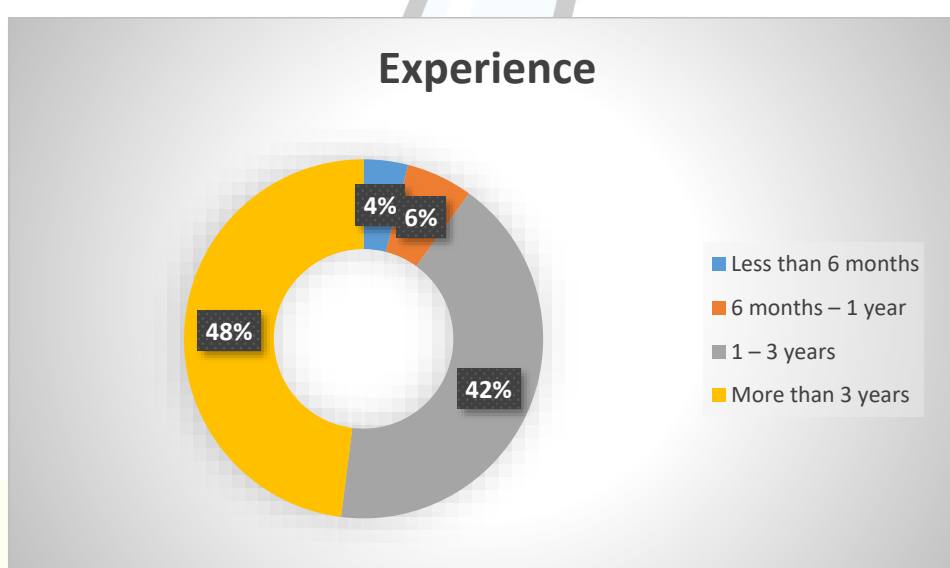
The majority of respondents (32%) fall within the ₹60,001–₹80,000 income bracket, followed closely by 28% earning above ₹80,000, indicating that fintech application users are largely from middle to upper-income households. This suggests a strong adoption of fintech services among financially stable individuals.

5. How long have you been using fintech applications?

Table no. 4.5

“Experience”	“No. of Respondents”	“Percentage”
“Less than 6 months”	4	4%
“6 months – 1 year”	6	6%
“1 – 3 years”	42	42%
“More than 3 years”	48	48%
“Total”	100	100%

Chart no. 4.5



Interpretation:

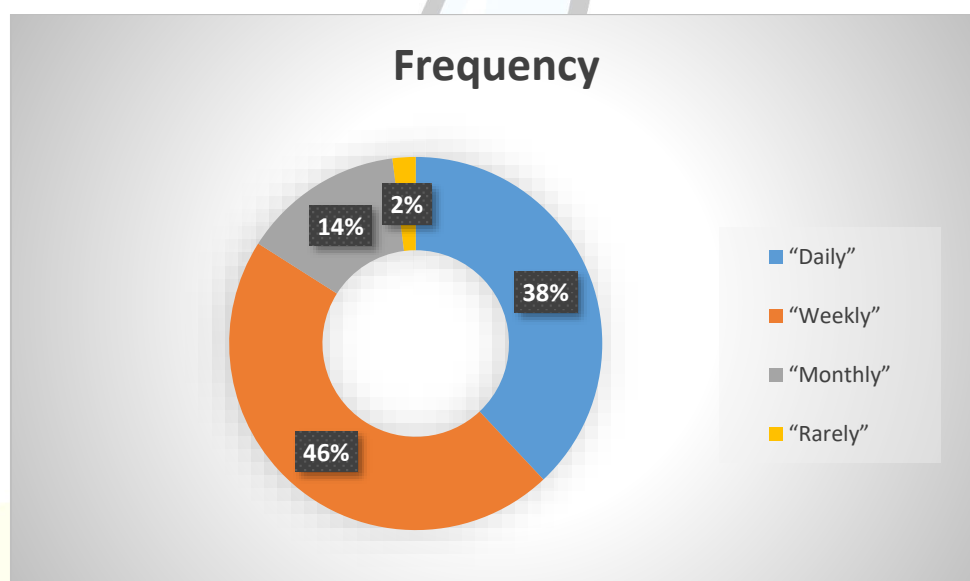
A significant portion of respondents have substantial experience with fintech applications, with 48% using them for more than 3 years and 42% for 1–3 years, indicating a mature and well-acquainted user base whose perceptions are shaped by long-term usage.

6. How frequently do you use fintech apps?

Table no. 4.6

“Frequency”	“No. of Respondents”	“Percentage”
“Daily”	38	38%
“Weekly”	46	46%
“Monthly”	14	14%
“Rarely”	2	2%
“Total”	100	100%

Chart no. 4.6



Interpretation:

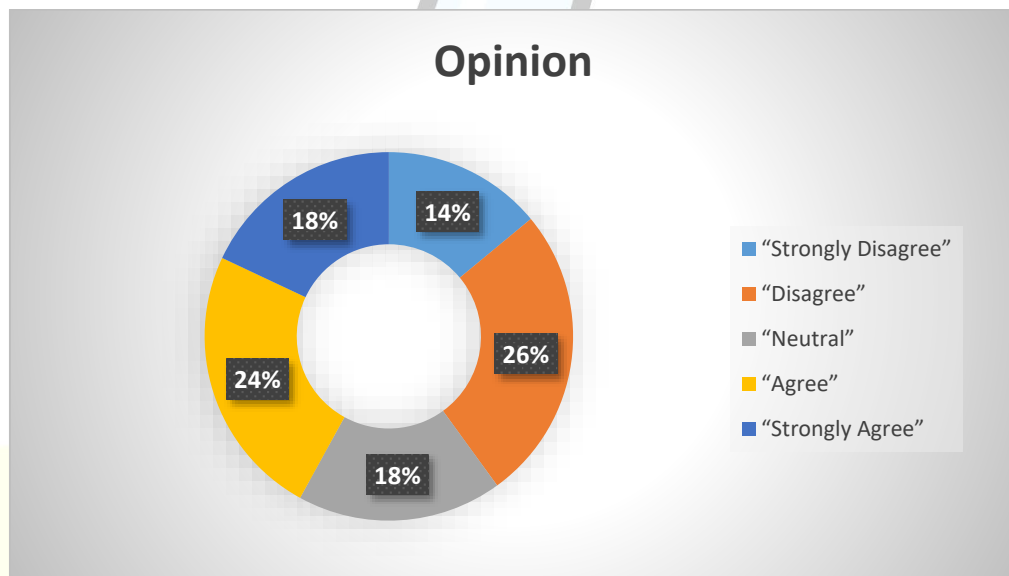
The majority of respondents use fintech apps frequently, with 46% using them weekly and 38% using them daily, highlighting a high level of engagement and reliance on these platforms for regular financial transactions.

7. I am aware of the data privacy policies of the fintech applications I use.

Table no. 4.7

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	14	14%
“Disagree”	26	26%
“Neutral”	18	18%
“Agree”	24	24%
“Strongly Agree”	18	18%
“Total”	100	100%

Chart no. 4.7



Interpretation:

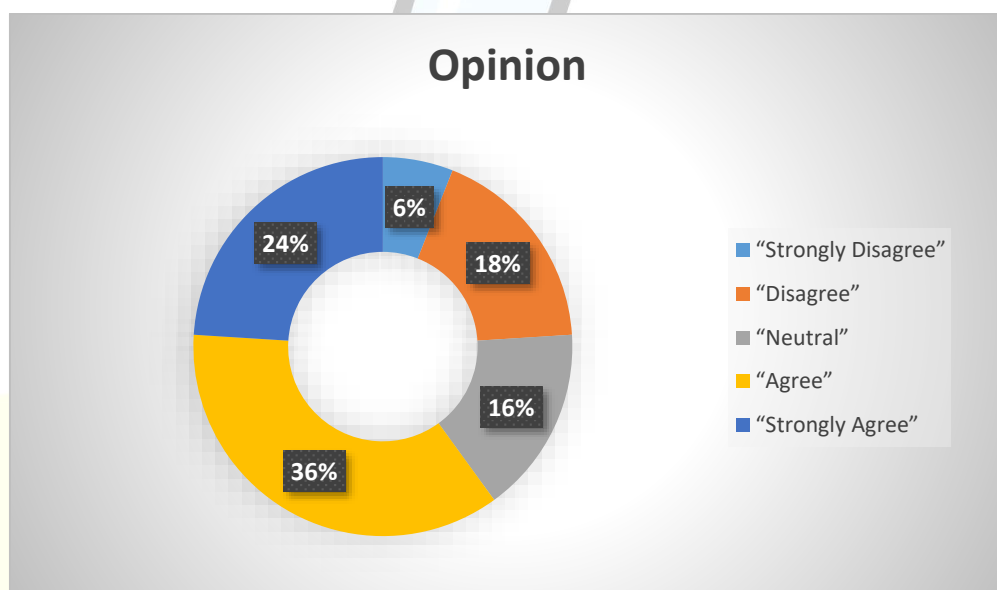
The responses indicate mixed awareness regarding data privacy policies in fintech apps, with 40% of users disagreeing or strongly disagreeing, while only 42% expressed agreement or strong agreement. This suggests that a considerable portion of users may be using these apps without fully understanding their privacy terms.

8. I understand the type of personal and financial data collected by fintech apps.

Table no. 4.8

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	6	6%
“Disagree”	18	18%
“Neutral”	16	16%
“Agree”	36	36%
“Strongly Agree”	24	24%
“Total”	100	100%

Chart no. 4.8



Interpretation:

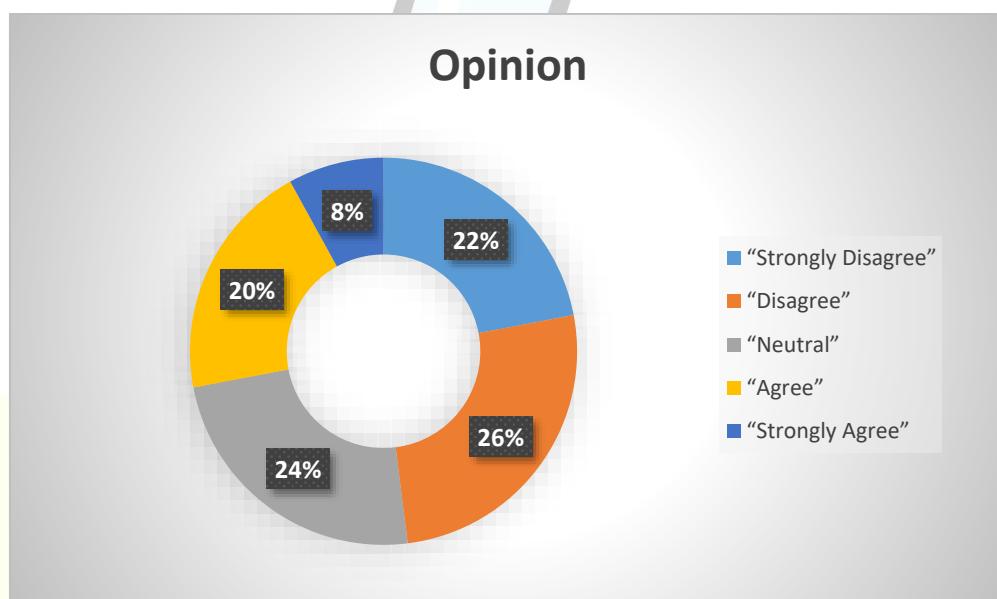
A majority of respondents (60%) agree or strongly agree that they understand the type of personal and financial data collected by fintech apps, indicating a relatively good level of user awareness, although 24% still show lack of clarity or uncertainty.

9. I regularly read the terms and conditions or privacy policies before using fintech apps.

Table no. 4.9

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	22	22%
“Disagree”	26	26%
“Neutral”	24	24%
“Agree”	20	20%
“Strongly Agree”	8	8%
“Total”	100	100%

Chart no. 4.9



Interpretation:

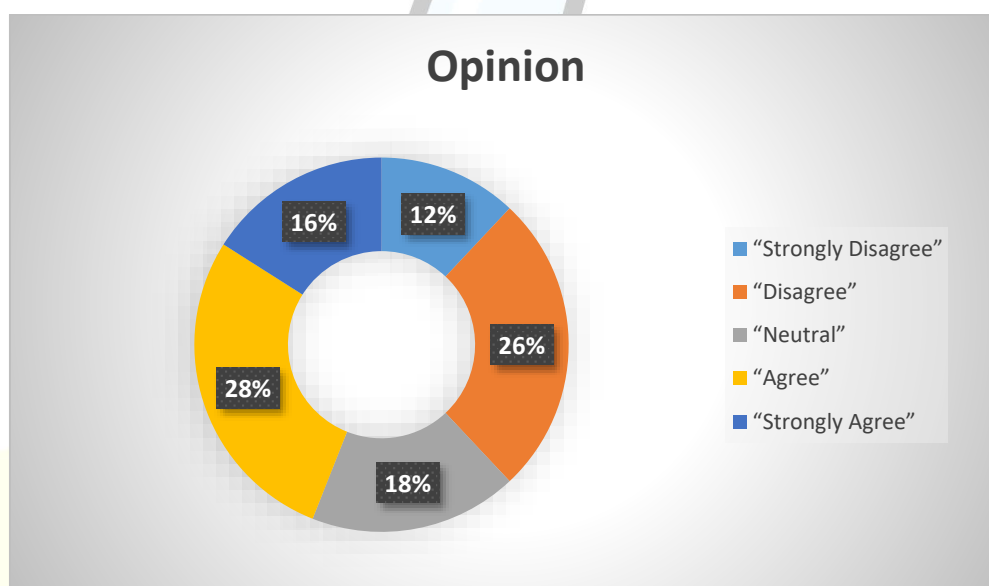
A large segment of respondents (48%) either disagree or strongly disagree with regularly reading terms and privacy policies, while only 28% claim to do so. This suggests that most users tend to overlook detailed privacy information before using fintech applications.

10. I am aware of how fintech apps use or share my data with third parties.

Table no. 4.10

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	12	12%
“Disagree”	26	26%
“Neutral”	18	18%
“Agree”	28	28%
“Strongly Agree”	16	16%
“Total”	100	100%

Chart no. 4.10



Interpretation:

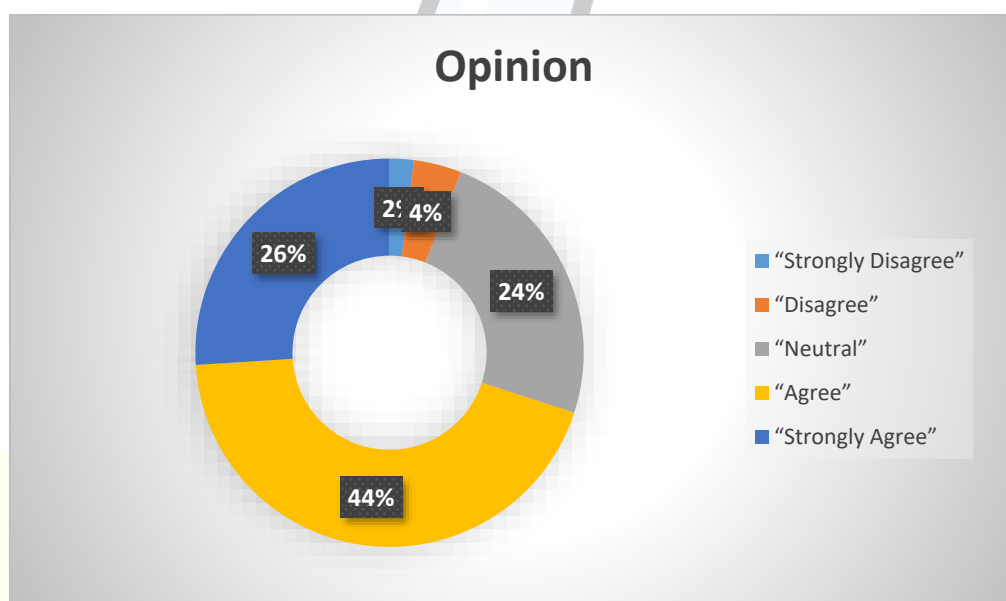
The responses show that 38% of users are not aware of how their data is shared with third parties, while 44% claim some level of awareness. This indicates a moderate knowledge gap among users regarding data-sharing practices of fintech apps.

11. I believe fintech applications have strong data security measures in place.

Table no. 4.11

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	4	4%
“Neutral”	24	24%
“Agree”	44	44%
“Strongly Agree”	26	26%
“Total”	100	100%

Chart no. 4.11



Interpretation:

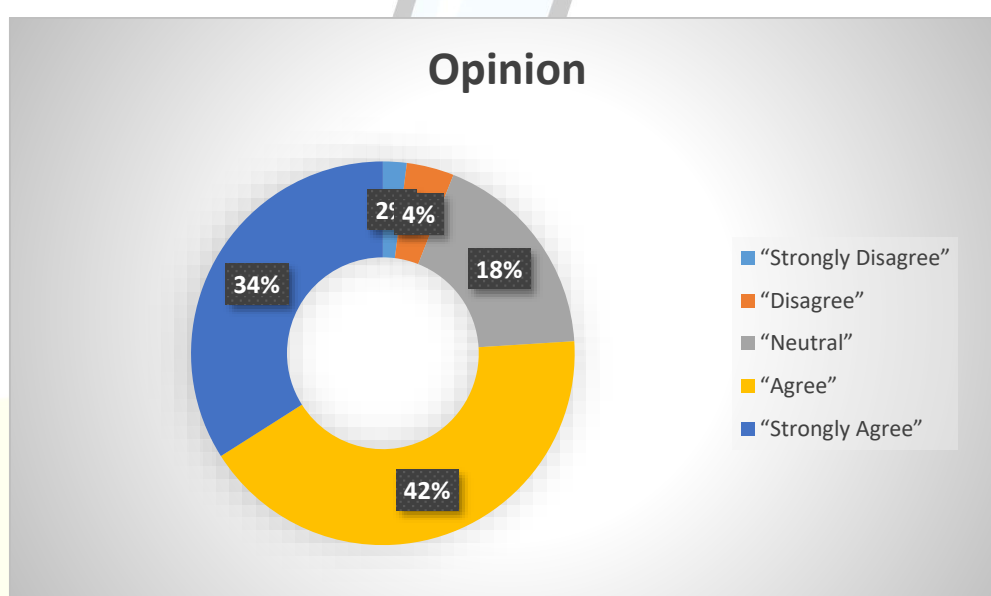
A majority of respondents (70%) agree or strongly agree that fintech applications have strong data security measures, reflecting a high level of confidence among users in the security infrastructure of these platforms.

12. The use of biometric login or two-factor authentication increases my trust in fintech apps.

Table no. 4.12

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	4	4%
“Neutral”	18	18%
“Agree”	42	42%
“Strongly Agree”	34	34%
“Total”	100	100%

Chart no. 4.12



Interpretation:

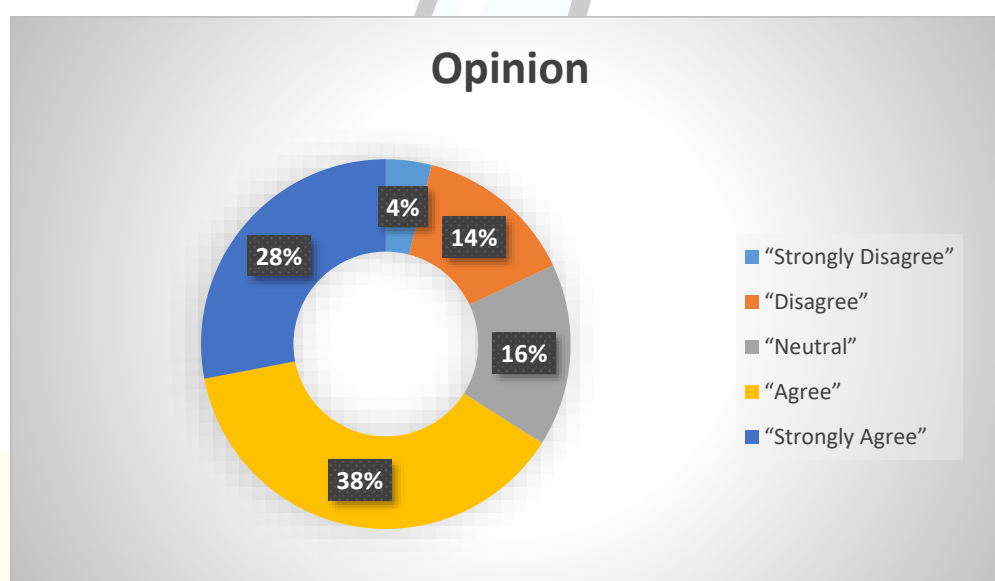
An overwhelming 76% of respondents agree or strongly agree that biometric login or two-factor authentication increases their trust in fintech apps, indicating that advanced security features play a crucial role in enhancing user confidence.

13. I feel secure when using fintech apps for financial transactions.

Table no. 4.13

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	4	4%
“Disagree”	14	14%
“Neutral”	16	16%
“Agree”	38	38%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.13



Interpretation:

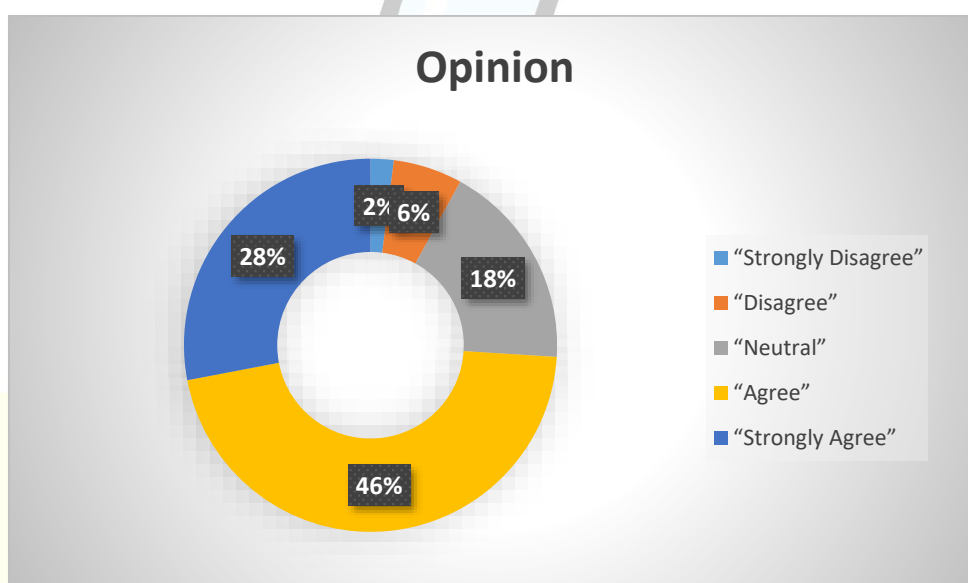
A significant majority of respondents (66%) feel secure when using fintech apps for financial transactions, while only 18% express insecurity, suggesting a generally positive perception of security among users.

14. I trust fintech apps to protect my personal and financial data from breaches.

Table no. 4.14

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	6	6%
“Neutral”	18	18%
“Agree”	46	46%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.14



Interpretation:

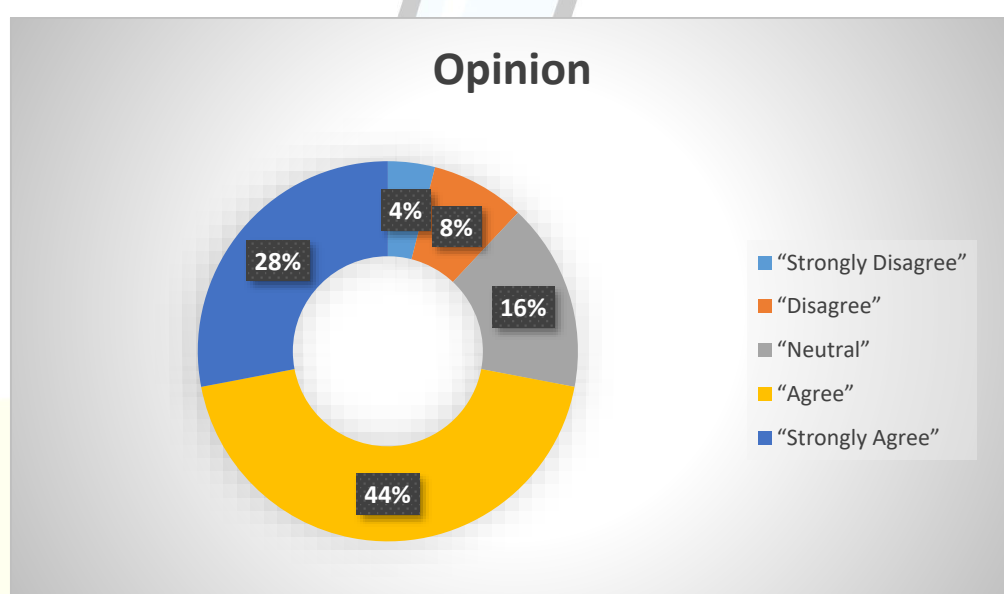
The data shows that 74% of respondents trust fintech apps to protect their personal and financial data, indicating strong user confidence in the platforms' ability to prevent data breaches.

15. I am concerned that my personal data might be misused by fintech companies.

Table no. 4.15

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	4	4%
“Disagree”	8	8%
“Neutral”	16	16%
“Agree”	44	44%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.15



Interpretation:

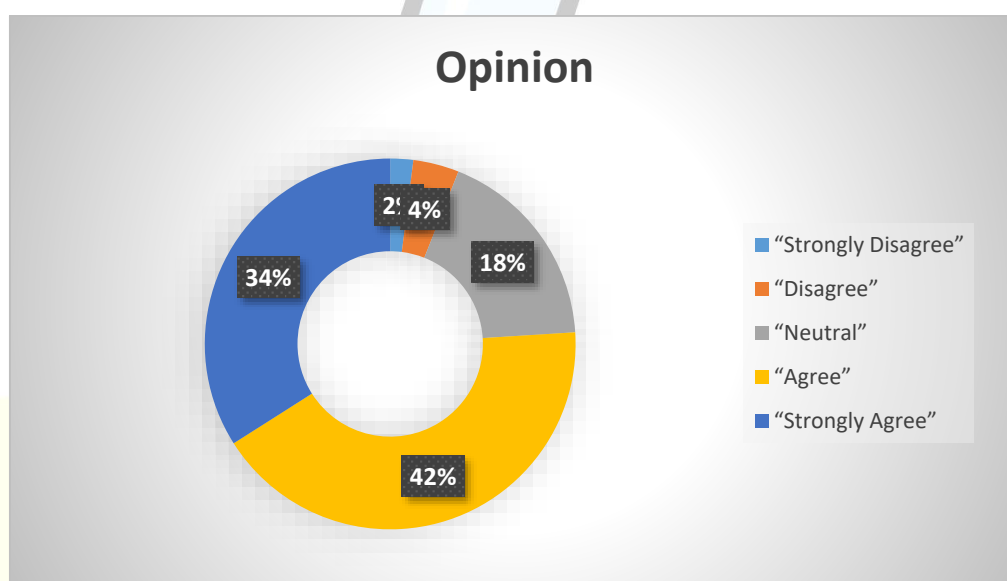
A combined 72% of respondents agree or strongly agree that they are concerned about the misuse of their personal data by fintech companies, highlighting a significant level of apprehension despite trust in security measures.

16. I worry about the possibility of data breaches or hacking in fintech platforms.

Table no. 4.16

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	4	4%
“Neutral”	18	18%
“Agree”	42	42%
“Strongly Agree”	34	34%
“Total”	100	100%

Chart no. 4.16



Interpretation:

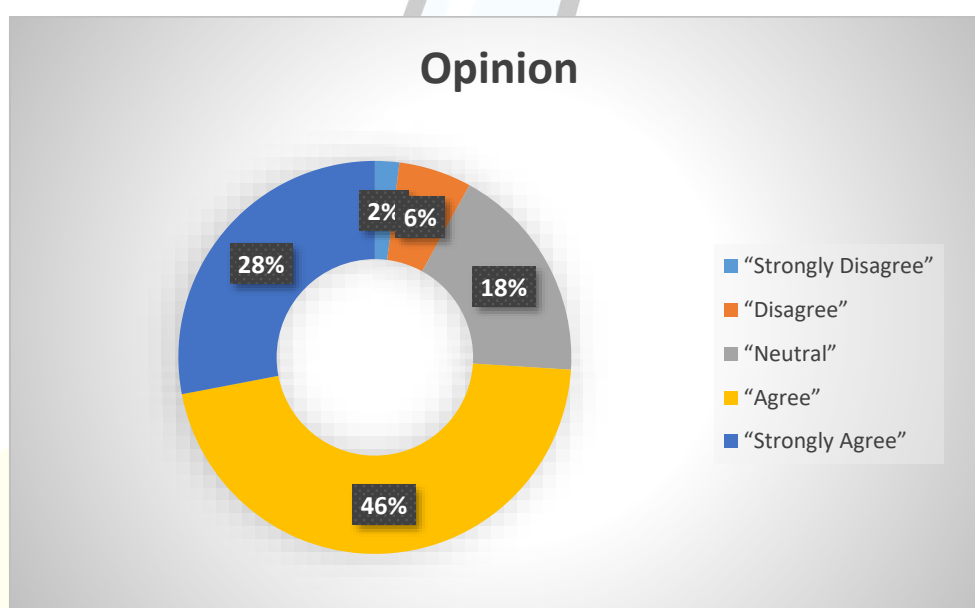
A substantial 76% of respondents express concern about data breaches or hacking on fintech platforms, indicating that security threats remain a key issue in users' minds despite advancements in protective measures.

17. I hesitate to use certain fintech features due to privacy concerns.

Table no. 4.17

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	6	6%
“Neutral”	18	18%
“Agree”	46	46%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.17



Interpretation:

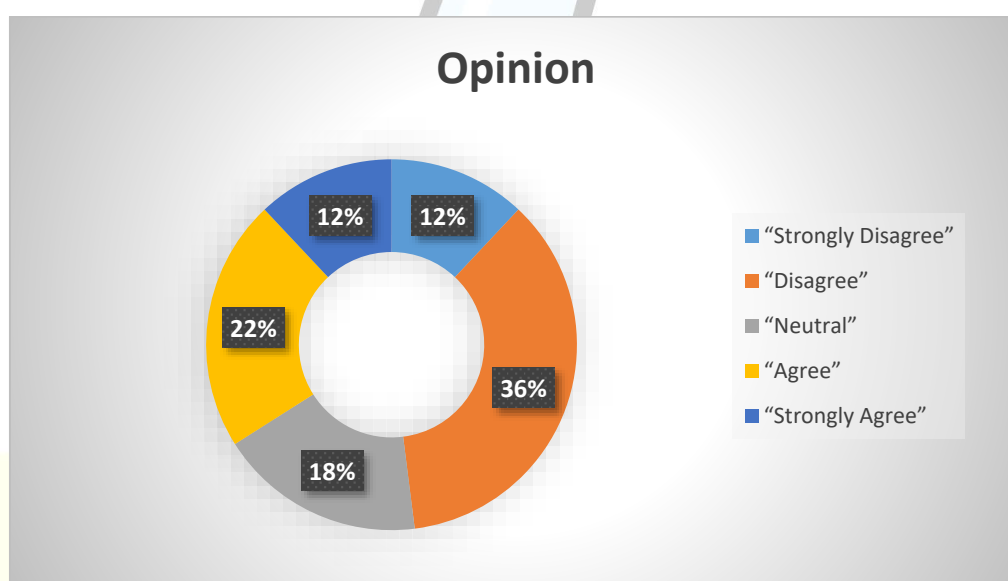
The majority of respondents (74%) admit to hesitating in using certain fintech features due to privacy concerns, suggesting that apprehensions about data handling significantly influence user behavior and feature adoption.

18. I have experienced or heard of security issues with fintech apps.

Table no. 4.18

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	12	12%
“Disagree”	36	36%
“Neutral”	18	18%
“Agree”	22	22%
“Strongly Agree”	12	12%
“Total”	100	100%

Chart no. 4.18



Interpretation:

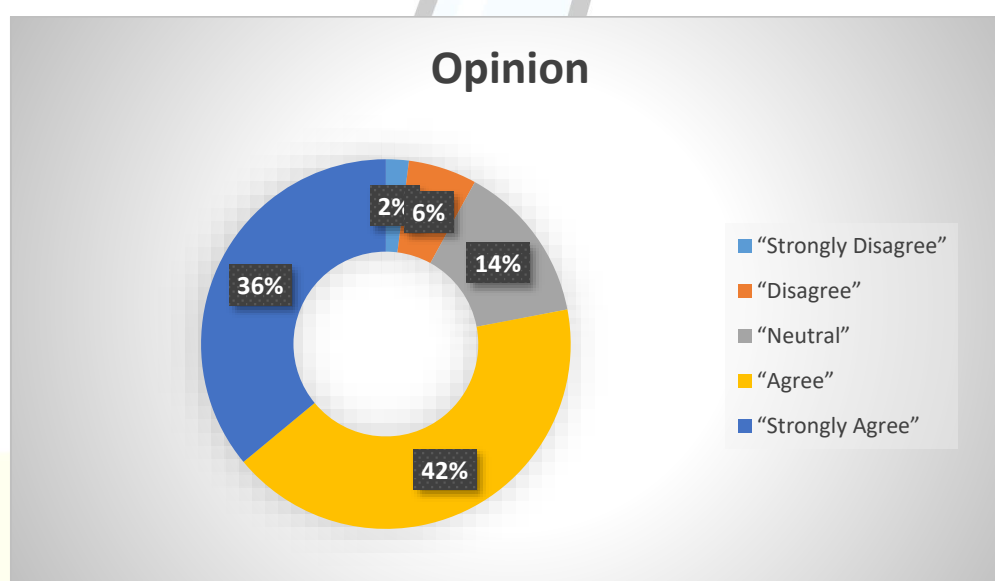
A combined 48% of respondents disagree or strongly disagree with having experienced or heard of security issues with fintech apps, while 34% have, indicating that although a majority have not encountered problems, a notable portion remains aware of potential security risks.

19. I limit the amount of personal information I share on fintech platforms.

Table no. 4.19

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	16	16%
“Neutral”	24	24%
“Agree”	32	32%
“Strongly Agree”	26	26%
“Total”	100	100%

Chart no. 4.19



Interpretation:

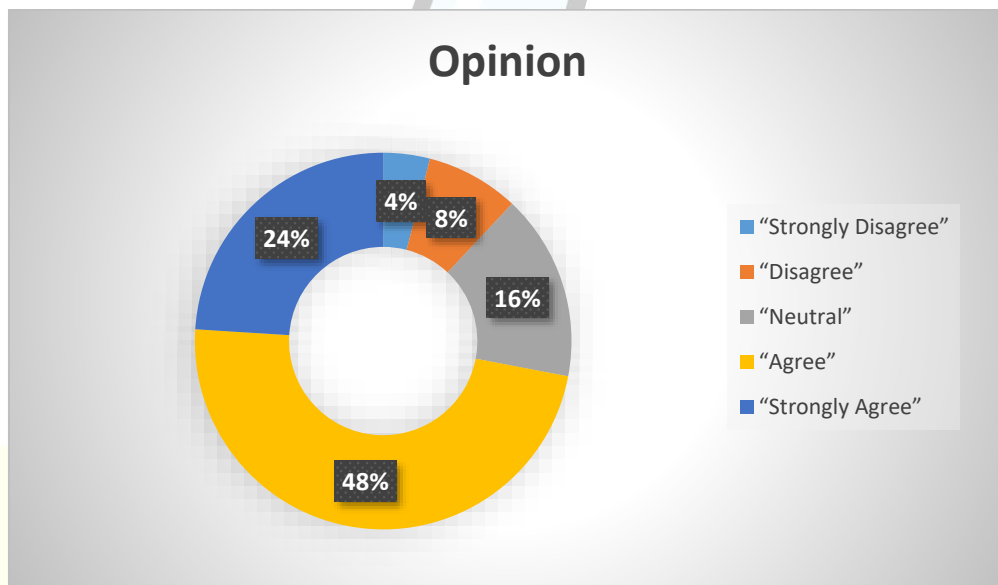
A majority of respondents (58%) agree or strongly agree that they limit the amount of personal information shared on fintech platforms, reflecting a cautious approach to data sharing driven by privacy concerns.

20. I choose fintech apps based on their reputation for data security.

Table no. 4.20

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	4	4%
“Disagree”	8	8%
“Neutral”	16	16%
“Agree”	48	48%
“Strongly Agree”	24	24%
“Total”	100	100%

Chart no. 4.20



Interpretation:

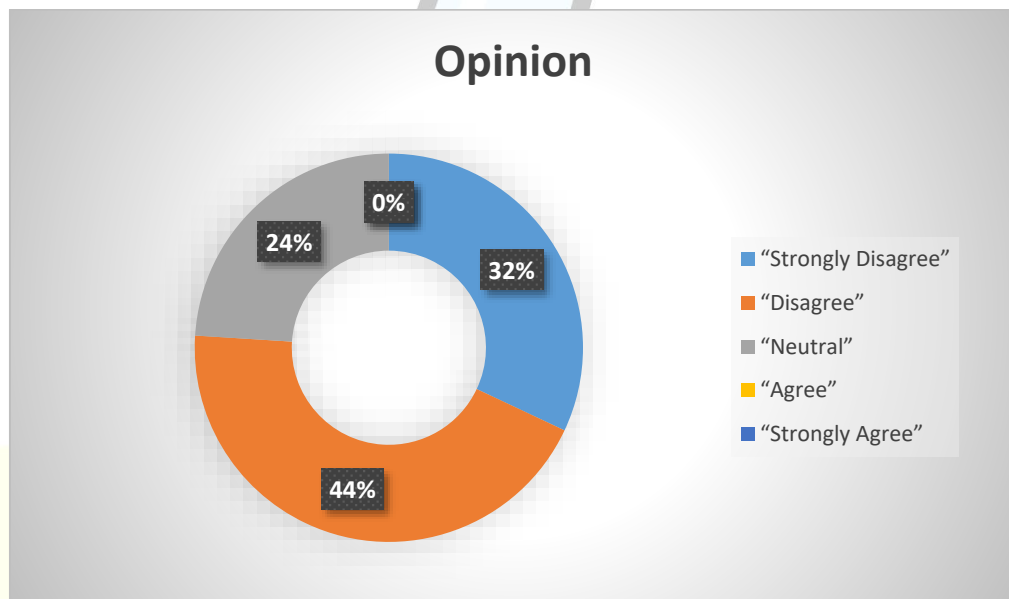
A strong majority of respondents (72%) agree or strongly agree that they choose fintech apps based on their reputation for data security, highlighting the importance of trust and perceived safety in user decision-making.

21. I stop using an app if I feel it compromises my data privacy.

Table no. 4.21

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	32	32%
“Disagree”	44	44%
“Neutral”	24	24%
“Agree”	0	0%
“Strongly Agree”	0	0%
“Total”	100	100%

Chart no. 4.21



Interpretation:

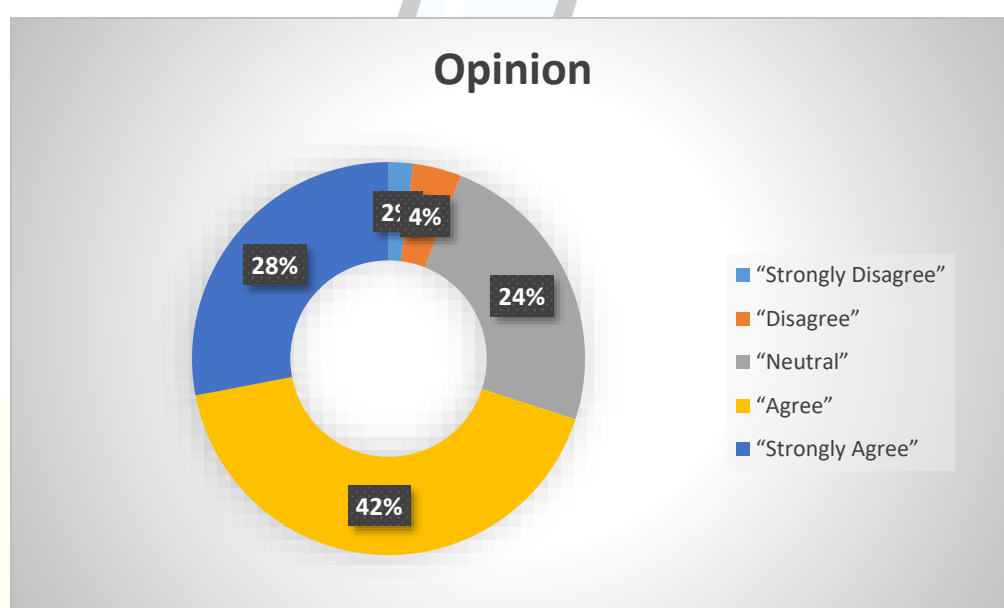
All respondents either disagreed (44%) or strongly disagreed (32%) with stopping the use of an app due to data privacy concerns, suggesting that despite privacy worries, most users continue using fintech apps, possibly due to convenience or lack of alternatives.

22. I am confident in the ability of fintech companies to handle my data responsibly.

Table no. 4.22

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	4	4%
“Neutral”	24	24%
“Agree”	42	42%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.22



Interpretation:

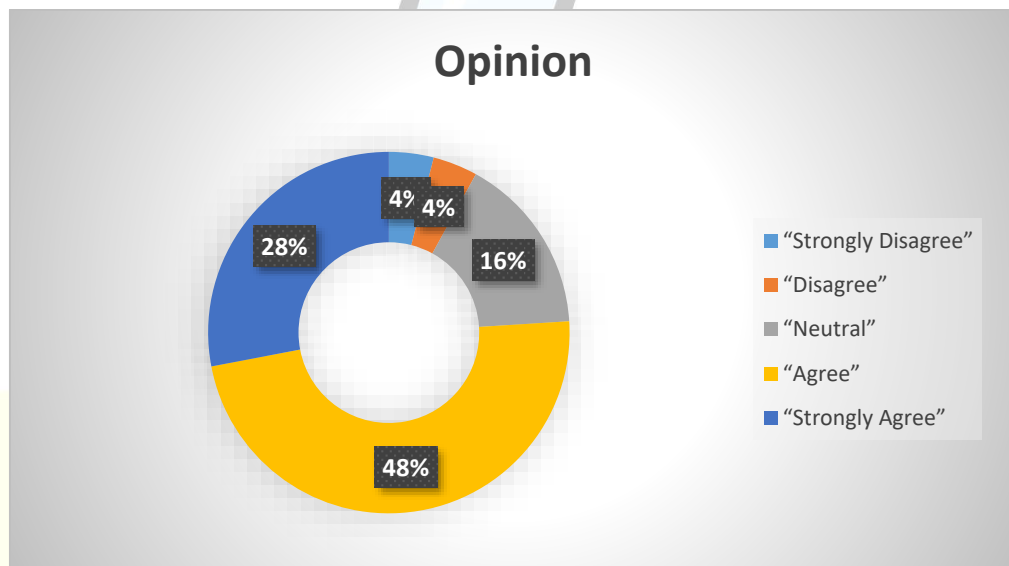
A significant majority of respondents (70%) express confidence in the ability of fintech companies to handle their data responsibly, indicating strong overall trust in the data management practices of these platforms.

23. My trust in fintech apps has increased over time due to better privacy measures.

Table no. 4.23

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	4	4%
“Disagree”	4	4%
“Neutral”	16	16%
“Agree”	48	48%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.23



Interpretation:

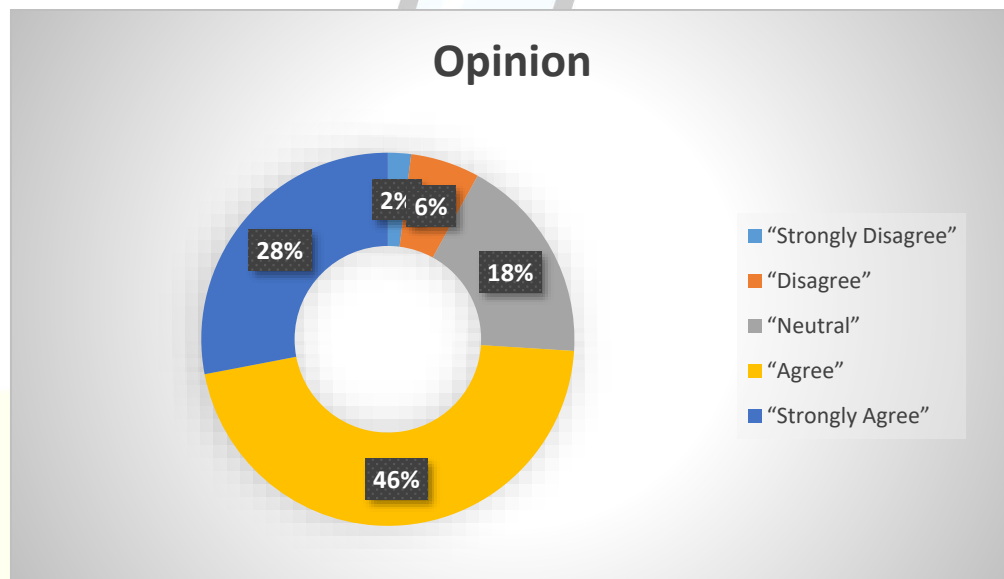
Most respondents (76%) agree or strongly agree that their trust in fintech apps has increased over time due to improved privacy measures, reflecting growing user confidence as security practices evolve.

24. Data privacy and security strongly influence my decision to use a fintech application.

Table no. 4.24

“Opinion”	“No. of Respondents”	“Percentage”
“Strongly Disagree”	2	2%
“Disagree”	6	6%
“Neutral”	18	18%
“Agree”	46	46%
“Strongly Agree”	28	28%
“Total”	100	100%

Chart no. 4.24



Interpretation:

A large majority of respondents (74%) agree or strongly agree that data privacy and security strongly influence their decision to use a fintech application, underscoring the critical role of trust and data protection in user adoption.

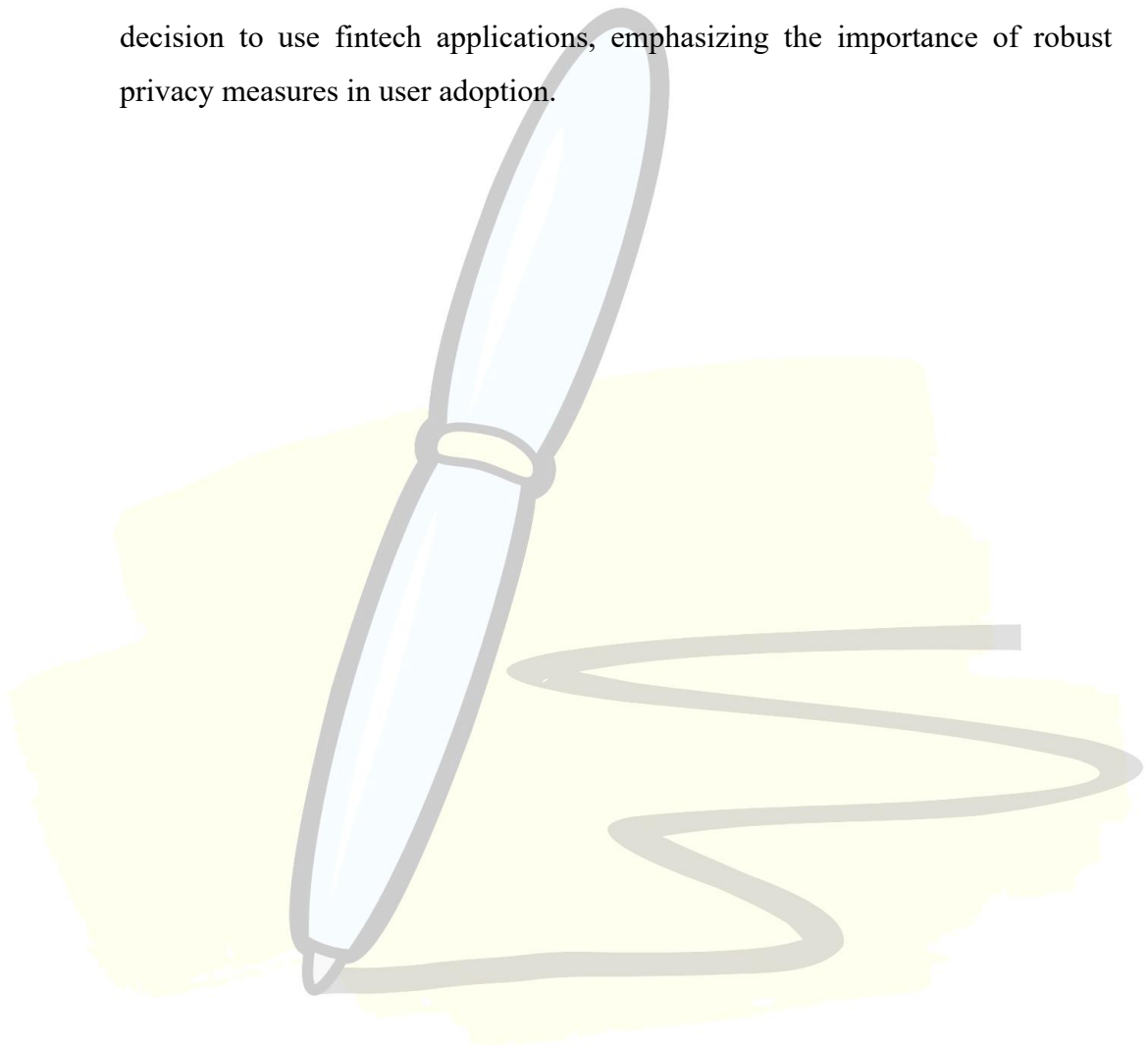
CHAPTER 5

FINDINGS, SUGGESTIONS, RECOMMENDATION

5.1. Findings of the Study:

- The study had an equal representation of male and female respondents, ensuring balanced gender perspectives on fintech usage and privacy concerns.
- A majority of users (54%) belong to the 21–30 years age group, indicating that young adults are the most engaged demographic with fintech applications.
- Most respondents are working professionals (44%), followed by students and self-employed individuals, suggesting broad adoption among economically active users.
- A significant portion (60%) of users belong to the middle to upper-income categories, reflecting that financially stable individuals are more inclined to use fintech services.
- The majority of users (90%) have been using fintech applications for over a year, with high frequency, indicating familiarity and consistent engagement with such platforms.
- Although 60% of users claim to understand the type of data collected, 40% are still unaware of privacy policies, and 48% admitted to not reading terms and conditions.
- Despite general trust, many users (72%) expressed concern over misuse of personal data, and 76% worry about potential data breaches or hacking.
- Advanced security features like biometric login and two-factor authentication are positively received, with 76% stating they increase trust in fintech apps.
- Most users (74%) trust fintech apps to protect their data, yet the same percentage admitted hesitating to use certain features due to privacy concerns.
- Nearly half of the respondents (48%) have not heard of security issues, while 34% have, indicating a mix of awareness and exposure to risks.

- While 72% of respondents consider data security reputation when choosing fintech apps, 76% have grown more confident in these apps over time due to improved privacy measures.
- Interestingly, despite privacy concerns, 76% of users do not stop using an app even if they feel it compromises their data, suggesting convenience outweighs caution for many users.
- Overall, 74% agree that data privacy and security strongly influence their decision to use fintech applications, emphasizing the importance of robust privacy measures in user adoption.



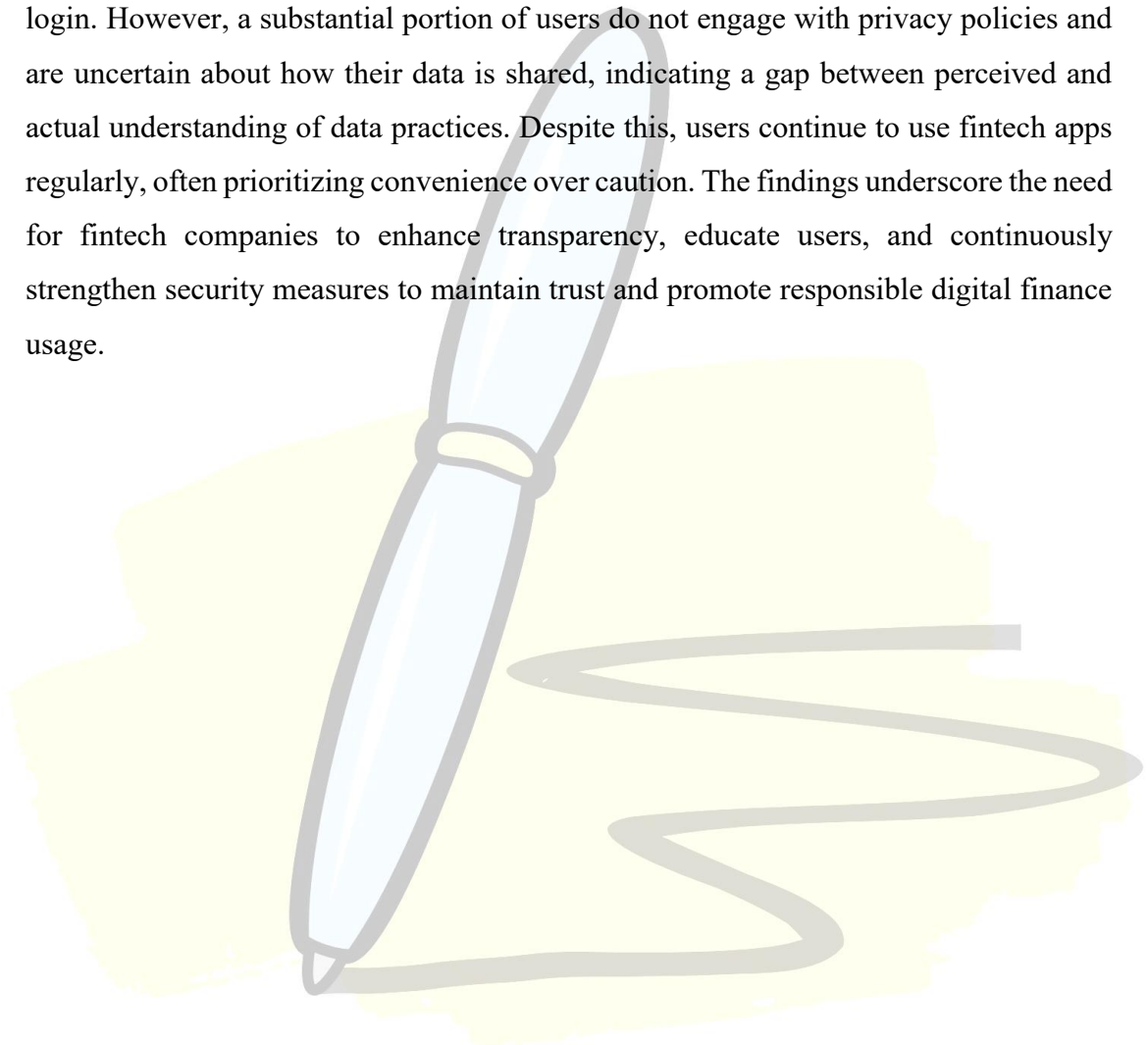
5.2. Suggestions:

- Fintech companies should simplify and highlight their privacy policies to improve user awareness and transparency.
- Regular security updates and visible privacy assurance messages can enhance user trust and reduce hesitation in using app features.
- Educating users through in-app tutorials or notifications about data usage and protection practices can bridge the awareness gap.
- Companies should emphasize the use of secure technologies like two-factor authentication and biometric verification as standard features.
- Prompt communication and support in the event of a data breach can help mitigate fear and retain user confidence.
- Fintech platforms should consider user feedback to continually improve security features and align them with user expectations.
- Greater emphasis should be placed on trust-building campaigns showcasing the company's commitment to data privacy and ethical data use.

CHAPTER 6

CONCLUSION

The study reveals that while fintech applications enjoy high levels of usage and trust among users, concerns regarding data privacy and security remain significant. Most users are aware of basic security features and express confidence in the platforms they use, particularly due to advancements like biometric authentication and two-factor login. However, a substantial portion of users do not engage with privacy policies and are uncertain about how their data is shared, indicating a gap between perceived and actual understanding of data practices. Despite this, users continue to use fintech apps regularly, often prioritizing convenience over caution. The findings underscore the need for fintech companies to enhance transparency, educate users, and continuously strengthen security measures to maintain trust and promote responsible digital finance usage.



BIBLIOGRAPHY

- [1] Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). *Data security, customer trust and intention for adoption of fintech services: An empirical analysis from commercial bank users in Pakistan*. SAGE Open, 13(3), 1–17. <https://doi.org/10.1177/21582440231181388>
- [2] Nangin, M. A., Barus, I. R. G., & Wahyoedi, S. (2020). *The effects of perceived ease of use, security, and promotion on trust and its implications on fintech adoption*. Journal of Consumer Sciences, 5(2), 124–138. <https://doi.org/10.29244/jcs.5.2.124-138>
- [3] Nayak, K., Singh, P., & Dave, P. (2021). *Does data security and trust affect the users of fintech?* International Journal of Management (IJM), 12(1), 191–206. <https://doi.org/10.34218/IJM.12.1.2021.016>
- [4] Dash, B., Sharma, P., & Ali, A. (2022). *Federated learning for privacy-preserving: A review of PII data analysis in fintech*. International Journal of Software Engineering & Applications (IJSEA), 13(4), 1–13. <https://doi.org/10.5121/ijsea.2022.13401>
- [5] Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). *Encryption techniques for financial data security in fintech applications*. International Journal of Science and Research Archive, 12(1), 2942–2949. <https://doi.org/10.30574/ijsra.2024.12.1.1210>
- [6] Abdul-Rahim, R., Bohari, S. A., Aman, A., & Awang, Z. (2022). *Benefit–risk perceptions of FinTech adoption for sustainability from bank consumers’ perspective: The moderating role of fear of COVID-19*. Sustainability, 14(14), 8357. <https://doi.org/10.3390/su14148357>
- [7] Yu, A.-P., Xu, C., & Cho, S.-E. (2024). *Factors affecting customer use intention of MyData services in the fintech industry*. Journal of Theoretical and Applied Electronic Commerce Research, 19(4), 3412–3428. <https://doi.org/10.3390/jtaer19040165>
- [8] Nguyen, D. D., Nguyen, T. D., Nguyen, T. D., & Nguyen, H. V. (2021). *Impacts of perceived security and knowledge on continuous intention to use mobile fintech payment services: An empirical study in Vietnam*. Journal of Asian Finance, Economics and Business, 8(8), 287–296. <https://doi.org/10.13106/jafeb.2021.vol8.no8.0287>

- [9] Dorfleitner, G., & Hornuf, L. (2019). *FinTech and data privacy in Germany: An empirical analysis with policy recommendations*. Springer. <https://doi.org/10.1007/978-3-030-31335-7>
- [10] Aldboush, H. H. H., & Ferdous, M. (2023). *Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust*. International Journal of Financial Studies, 11(3), 90. <https://doi.org/10.3390/ijfs11030090>
- [11] Juma'h, A., Alnsour, Y., & Kartal, H. (2025). *Perceived security and privacy in cryptocurrency apps: A text mining and ordinal regression approach*. Journal of Theoretical and Applied Electronic Commerce Research, 20(1), 1–17. <https://doi.org/10.3390/jtaer20010002>
- [12] Wijaya, I. D., Astuti, E. S., Yulianto, E., & Abdillah, Y. (2025). *Examining the impact of perceived usefulness on micro-entrepreneurs' intentions to use Fintech peer-to-peer lending applications with perceived security as a mediating factor*. Multidisciplinary Science Journal, 7, e2025483. <https://doi.org/10.31893/multiscience.2025483>
- [13] Roh, T., Yang, Y. S., Xiao, S., & Park, B. I. (2022). *What makes consumers trust and adopt fintech? An empirical investigation in China*. Electronic Commerce Research, 24, 3–35. <https://doi.org/10.1007/s10660-021-09527-3>
- [14] Laurent, D., & Sinz, R. (2019). *FinTech: The role of perceived cybersecurity and organizational trust—Investigating from a customer perspective in Sweden* (Master's thesis, Umeå University). <https://www.diva-portal.org/smash/get/diva2:1329050/FULLTEXT01.pdf>
- [15] Wang, J. S. (2021). *Exploring biometric identification in FinTech applications based on the modified TAM*. Financial Innovation, 7(42), 1–18. <https://doi.org/10.1186/s40854-021-00260-2>
- [16] AlHassan, H. A., Papastathopoulos, A., & Nobanee, H. (2025). *Measuring perceived security in FinTech services: Developing a dynamic scale*. Journal of Business Research, 173, 114021. <https://doi.org/10.1016/j.jbusres.2023.114021>
- [17] Jafri, J. A., Mohd Amin, S. I., Abdul Rahman, A., & Mohd Nor, S. (2024). *A systematic literature review of the role of trust and security on*

- FinTech adoption in banking.* Heliyon, 10, e22980.
<https://doi.org/10.1016/j.heliyon.2023.e22980>
- [18] Hwang, Y., Park, S., & Shin, N. (2021). *Sustainable development of a mobile payment security environment using FinTech solutions.* Sustainability, 13(15), 8375. <https://doi.org/10.3390/su13158375>
- [19] Ali, M., Raza, S. A., Khamis, B., Puah, C.-H., & Amin, H. (2021). *How perceived risk, benefit and trust determine user FinTech adoption: A new dimension for Islamic finance.* Foresight, 23(6), 607–623.
<https://doi.org/10.1108/FS-09-2020-0095>
- [20] Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2023). *Promise not fulfilled: FinTech, data privacy, and the GDPR.* Electronic Markets, 33, 33.
<https://doi.org/10.1007/s12525-023-00622-x>
- [21] Singh, S., Sahni, M. M., & Kovid, R. (2020). *What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model.* Information Systems Frontiers, 23, 457–478.
<https://doi.org/10.1007/s10796-020-10064-x>
- [22] Bouteraa, M., Chekima, B., Lajuni, N., & Anwar, A. (2023). *Understanding consumers' barriers to using FinTech services in the United Arab Emirates: Mixed-methods research approach.* Journal of Financial Services Marketing, 28, 215–229. <https://doi.org/10.1057/s41264-023-00179-4>
- [23] Vasquez, O., & San-Jose, L. (2022). *Ethics in FinTech through users' confidence: Determinants that affect trust.* Ramon Llull Journal of Applied Ethics, 13, 99–149. <https://doi.org/10.34810/rljaev1n13Id398681>
- [24] Alwi, S., Alpandi, R. M., Salleh, M. N. M., Basir, I. N., & Md Ariff, F. F. (2019). *An empirical study on the customers' satisfaction on FinTech mobile payment services in Malaysia.* International Journal of Advanced Science and Technology, 28(16), 390–400.
- [25] Osman, Z., Razli, I. A., & Ing, P. (2021). *Does security concern, perceived enjoyment and government support affect FinTech adoption? Focused on bank users.* Journal of Marketing Advances and Practices, 3(1), 62–74.
- [26] Alalwan, A. A., Baabdullah, A. M., Al-Debei, M. M., Raman, R., Alhitmi, H. K., Abu-ElSamen, A. A., & Dwivedi, Y. K. (2023). *Fintech and contactless payment: Help or hindrance? The role of invasion of privacy and*

information disclosure. Information Technology & People.
<https://doi.org/10.1108/ITP-04-2022-0286>

- [27] Chan, R., Troshani, I., Hill, S. R., & Hoffmann, A. (2022). *Towards an understanding of consumers' FinTech adoption: The case of Open Banking*. Computers in Human Behavior, 134, 107321.
<https://doi.org/10.1016/j.chb.2022.107321>
- [28] Al Nawayseh, M. K. (2020). *FinTech in COVID-19 and beyond: What factors are affecting customers' choice of FinTech applications?* Journal of Open Innovation: Technology, Market, and Complexity, 6(4), 153.
<https://doi.org/10.3390/joitmc6040153>
- [29] Juma'h, A., Alnsour, Y., & Kartal, H. (2025). *The impact of security and privacy perceptions on cryptocurrency app evaluations by users: A text mining study*. Investment Management and Financial Innovations, 22(1), 173–187.
[https://doi.org/10.21511/imfi.22\(1\).2025.14](https://doi.org/10.21511/imfi.22(1).2025.14)
- [30] Gai, K., Qiu, M., & Sun, X. (2018). *A survey on FinTech*. Journal of Network and Computer Applications, 103, 262–273.
<https://doi.org/10.1016/j.jnca.2017.10.011>
- [31] Li, C., Khaliq, N., Chinove, L., Khaliq, U., & Oláh, J. (2023). *Consumers' perception of risk facets associated with FinTech use: Evidence from Pakistan*. Risks, 11(5), 89. <https://doi.org/10.3390/risks11050089>
- [32] Meyliana, Fernando, E., & Surjandy. (2019). *The influence of perceived risk and trust in adoption of FinTech services in Indonesia*. International Journal of Advanced Computer Science and Applications, 10(11), 351–359.
<https://doi.org/10.14569/IJACSA.2019.0101142>
- [33] Appiah, T., & Agblewornu, V. V. (2025). *The interplay of perceived benefit, perceived risk, and trust in FinTech adoption: Insights from Sub-Saharan Africa*. Information Systems Frontiers.
<https://doi.org/10.1007/s10796-025-10358-2>
- [34] Nigam, A., Khan, F. S., Mazhar, S. S., Chaudhary, N., Haque, E., Mir, M. A., & Ansari, M. S. (2024). *Consumer perceptions and attitudes towards e-payment services offered by FinTech companies: Evidence from India*. Journal of Infrastructure, Policy and Development, 8(11), 7522.
<https://doi.org/10.24294/jipd.v8i11.7522>

- [35] Meng, W., Zhu, L., Li, W., Han, J., & Li, Y. (2019). *Enhancing the security of FinTech applications with map-based graphical password authentication*. *Future Generation Computer Systems*, 101, 1018–1027. <https://doi.org/10.1016/j.future.2019.07.012>
- [36] Ryu, H.-S., & Ko, K. S. (2020). *Sustainable development of Fintech: Focused on uncertainty and perceived quality issues*. *Sustainability*, 12(21), 8881. <https://doi.org/10.3390/su12218881>
- [37] Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). *Data privacy laws and their impact on financial technology companies: A review*. *Journal of Financial Regulation and Compliance*, 32(1), 45–59. <https://doi.org/10.1108/JFRC-06-2023-0112>
- [38] Akmal, S., Talha, M., Faisal, S. M., Ahmad, M., & Khan, A. K. (2023). *Perceptions about FinTech: New evidences from the Middle East*. *Journal of Financial Services Marketing*, 28(3), 249–261. <https://doi.org/10.1057/s41264-023-00181-w>
- [39] Aboalsamh, H. M., Khrais, L. T., & Albahussain, S. A. (2023). *Pioneering perception of green FinTech in promoting sustainable digital services application within smart cities*. *Sustainability*, 15(14), 11440. <https://doi.org/10.3390/su151411440>
- [40] Suryono, R. R., Budi, I., & Purwandari, B. (2021). *Detection of Fintech P2P lending issues in Indonesia*. *Heliyon*, 7(4), e06782. <https://doi.org/10.1016/j.heliyon.2021.e06782>

ANNEXURE

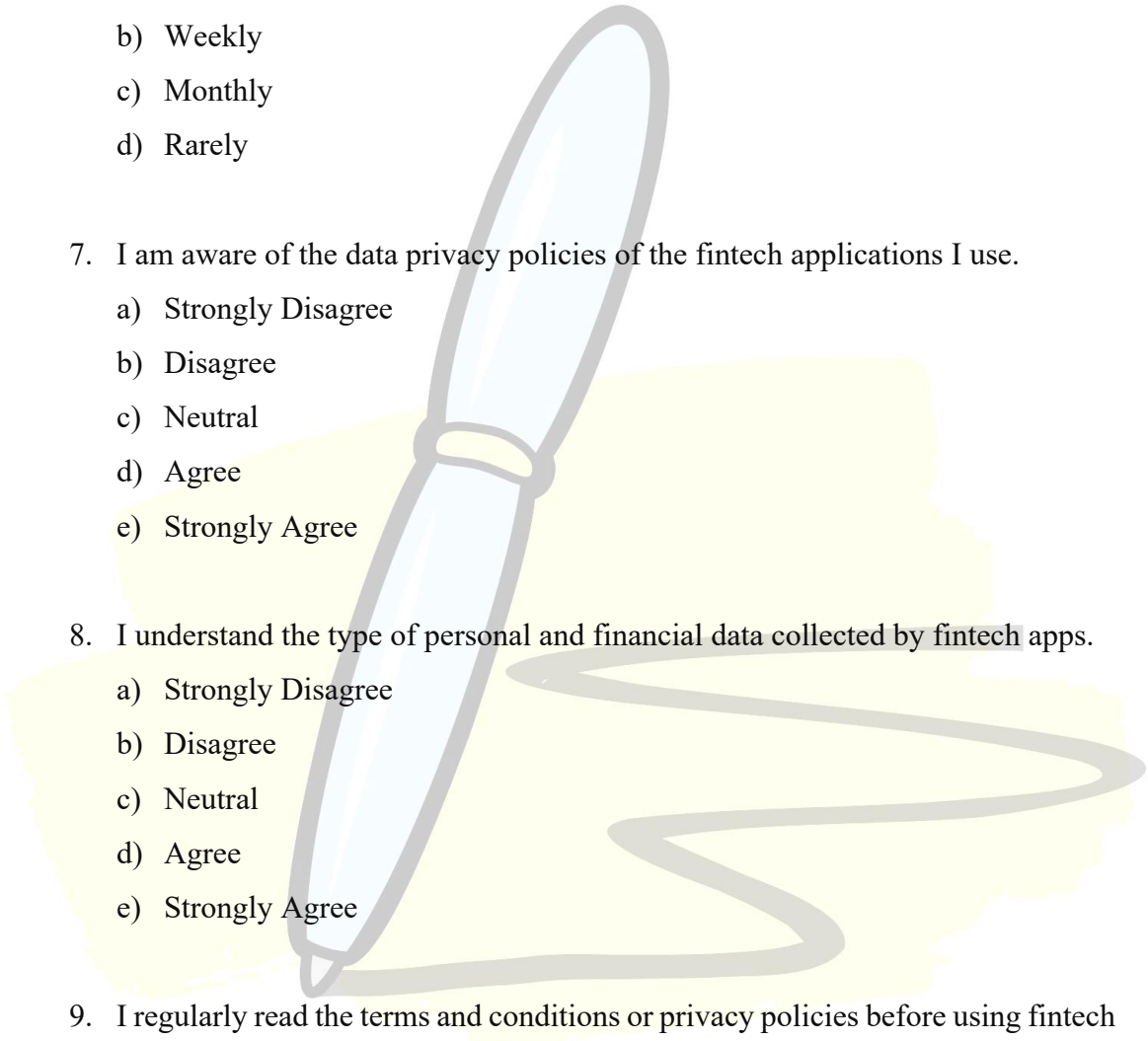
QUESTIONNAIRE

1. Gender:
 - a) Male
 - b) Female

2. Age Group:
 - a) Below 20 Years
 - b) 21 – 30 Years
 - c) 31 – 40 Years
 - d) 41 – 50 Years
 - e) Above 50 Years

3. Occupation:
 - a) Student
 - b) Working Professional
 - c) Self-employed
 - d) Homemaker
 - e) Retired
 - f) Others

4. Monthly Income:
 - a) Less than ₹20,000
 - b) ₹20,001 – ₹40,000
 - c) ₹40,001 – ₹60,000
 - d) ₹60,001 – ₹80,000
 - e) Above ₹80,000

- 
5. How long have you been using fintech applications?
- a) Less than 6 months
 - b) 6 months – 1 year
 - c) 1 – 3 years
 - d) More than 3 years
6. How frequently do you use fintech apps?
- a) Daily
 - b) Weekly
 - c) Monthly
 - d) Rarely
7. I am aware of the data privacy policies of the fintech applications I use.
- a) Strongly Disagree
 - b) Disagree
 - c) Neutral
 - d) Agree
 - e) Strongly Agree
8. I understand the type of personal and financial data collected by fintech apps.
- a) Strongly Disagree
 - b) Disagree
 - c) Neutral
 - d) Agree
 - e) Strongly Agree
9. I regularly read the terms and conditions or privacy policies before using fintech apps.
- a) Strongly Disagree
 - b) Disagree
 - c) Neutral
 - d) Agree
 - e) Strongly Agree

10. I am aware of how fintech apps use or share my data with third parties.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

11. I believe fintech applications have strong data security measures in place.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

12. The use of biometric login or two-factor authentication increases my trust in fintech apps.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

13. I feel secure when using fintech apps for financial transactions.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

14. I trust fintech apps to protect my personal and financial data from breaches.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree

e) Strongly Agree

15. I am concerned that my personal data might be misused by fintech companies.

a) Strongly Disagree

b) Disagree

c) Neutral

d) Agree

e) Strongly Agree

16. I worry about the possibility of data breaches or hacking in fintech platforms.

a) Strongly Disagree

b) Disagree

c) Neutral

d) Agree

e) Strongly Agree

17. I hesitate to use certain fintech features due to privacy concerns.

a) Strongly Disagree

b) Disagree

c) Neutral

d) Agree

e) Strongly Agree

18. I have experienced or heard of security issues with fintech apps.

a) Strongly Disagree

b) Disagree

c) Neutral

d) Agree

e) Strongly Agree

19. I limit the amount of personal information I share on fintech platforms.

a) Strongly Disagree

b) Disagree

c) Neutral

- d) Agree
- e) Strongly Agree

20. I choose fintech apps based on their reputation for data security.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

21. I stop using an app if I feel it compromises my data privacy.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

22. I am confident in the ability of fintech companies to handle my data responsibly.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

23. My trust in fintech apps has increased over time due to better privacy measures.

- a) Strongly Disagree
- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree

24. Data privacy and security strongly influence my decision to use a fintech application.

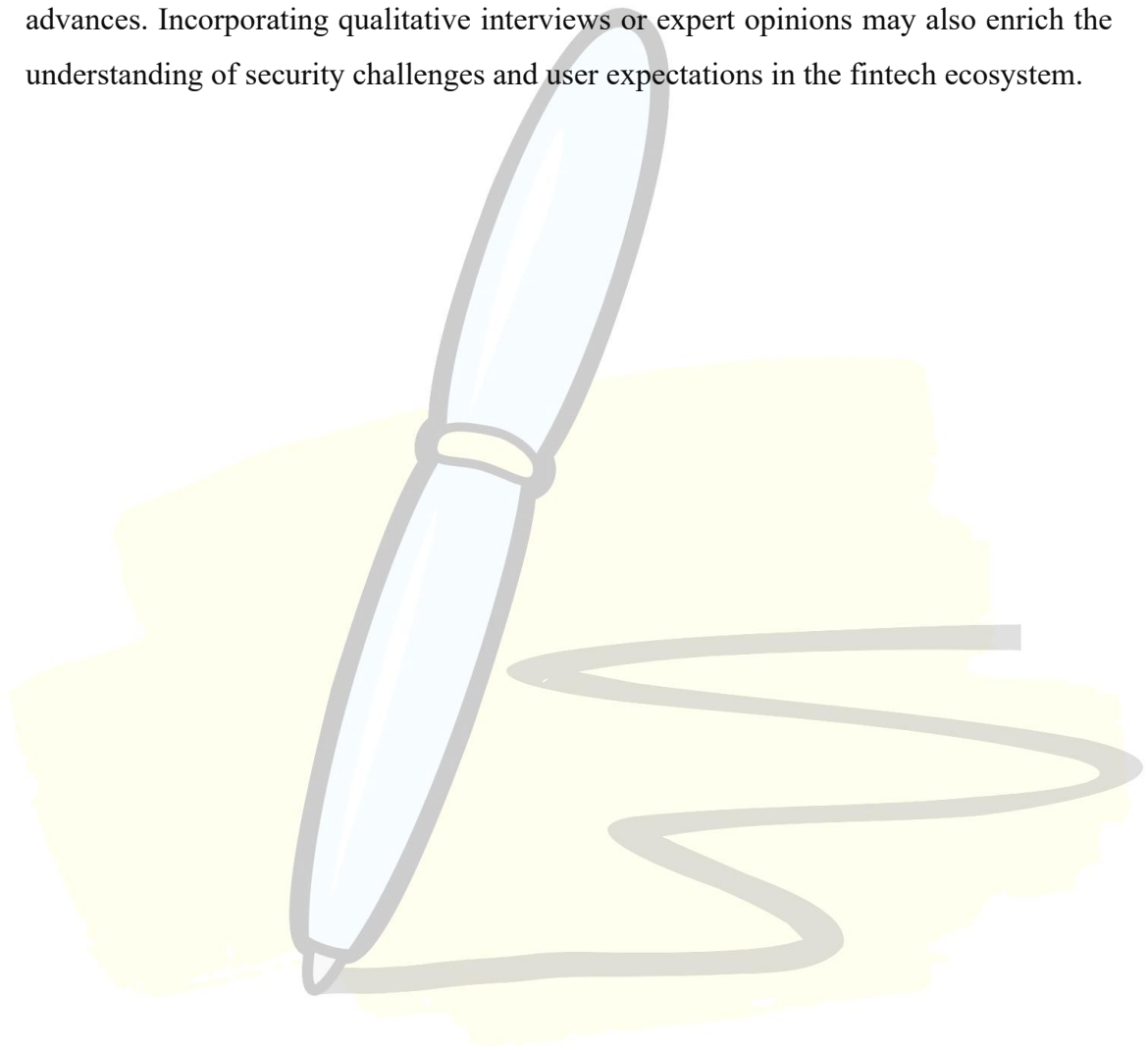
- a) Strongly Disagree

- b) Disagree
- c) Neutral
- d) Agree
- e) Strongly Agree



Scope for Future Study:

Future studies can explore user perception of data privacy and security across different regions or countries to identify cultural or regulatory influences. Comparative studies between various categories of fintech services—such as digital wallets, lending platforms, and investment apps—can offer deeper insights into trust factors unique to each segment. Additionally, longitudinal research could track changes in user awareness and behavior over time as privacy regulations evolve and technology advances. Incorporating qualitative interviews or expert opinions may also enrich the understanding of security challenges and user expectations in the fintech ecosystem.



PLAGIARISM REPORT

A Study on User Perception of Data Privacy and Security in
Fintech Applications.docx

ORIGINALITY REPORT

9%

SIMILARITY INDEX

10%

INTERNET SOURCES

6%

PUBLICATIONS

6%

STUDENT PAPERS

PRIMARY SOURCES

1

www.mdpi.com

Internet Source

1%

2

Submitted to Liverpool John Moores
University

Student Paper

1%

3

Submitted to Manipal University

Student Paper

1%

4

Submitted to University of Strathclyde

Student Paper

1%

5

fastercapital.com

Internet Source

<1%

6

gitarattan.edu.in

Internet Source

<1%

7

Wenxiang Zhang, Saeed Siyal, Samina Riaz,
Riaz Ahmad, Mohd Faiz Hilmi, Zhi Li. "Data
Security, Customer Trust and Intention for
Adoption of Fintech Services: An Empirical
Analysis From Commercial Bank Users in
Pakistan", SAGE Open, 2023

Publication

<1%

8

Submitted to Visvesvaraya Technological
University, Belagavi

Student Paper

<1%

9

pcte.edu.in

Internet Source

<1%