IJTBI
International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

A STUDY ON MOBILE BANKING SECURITY AWARENESS IN INDIA WITH REFERENCE TO BSNL

[#1]**Ms. A. JYOTHSNA,** ***Assistant Professor,***
[#2]**MADDI BHAVITHA,** ***PG Student,***
Department of MBA,
J.B. INSTITUTE OF ENGINEERING & TECHNOLOGY (AUTONOMOUS), HYDERABAD.

ABSTRACT: This research primarily focuses on BSNL and studies mobile banking security awareness in India, investigating consumers' views, knowledge gaps, and behavioral patterns about the protection of digital financial transactions. The research investigates the swift adoption of mobile banking across diverse demographics and the influence of BSNL's status as a prominent telecom provider on consumer security. The research employs primary data from surveys and relevant secondary sources to identify the principal elements affecting security awareness, including digital literacy, perceived risk, trust in service providers, and exposure to fraud prevention communications. The results indicate significant variability in clients' understanding of security protocols. This necessitates improved identification verification systems, targeted awareness initiatives, and more collaboration between telecommunications firms and financial institutions. The paper concludes with recommendations for enhancing the security of mobile banking in India and strengthening client resilience against attacks.

Keywords: *Mobile Banking Security, Security Awareness, BSNL, Digital Financial Literacy, Cybersecurity, User Perception, Telecom Service Providers, Mobile Banking Adoption, India, Fraud Prevention, Authentication Mechanisms, Data Protection.*

1. INTRODUCTION

In India, it is imperative to use caution to safeguard your mobile banking activities. This involves employing verified applications, activating multi-factor authentication, and refraining from conducting transactions on public Wi-Fi. Users must never disclose passwords, PINs, or one-time passwords (OTPs). Furthermore, they must be vigilant for phishing attempts manifesting as fraudulent emails or messages. To protect your personal data and avert fraud, it is essential to monitor account activity, remain aware of prevalent threats, and routinely update your software.

Mobile banking has transformed the financial management practices of individuals in India. They can utilize their mobile devices to efficiently, effortlessly, and reliably access a range of financial services. Inexpensive internet access is becoming increasingly prevalent, and digitalization is advancing swiftly. Consequently, millions of individuals are progressively using mobile phones for financial activities, bill payments, and money transfers. Major financial institutions and telecommunications firms, like BSNL, have facilitated this transformation by promoting digital banking services and improving mobile connection. The transition to digital

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

banking has facilitated access for everybody, especially in rural and semi-urban regions where conventional banks are limited.

Mobile Banking Security Awareness

- **Use strong and unique passwords:** Consumers ought to frequently update their passwords and refrain from utilizing easily discernible information.
- **Enable multi-factor authentication (MFA):** Biometrics or one-time passwords (OTPs) offer an additional degree of protection.
- **Avoid public Wi-Fi:** Engaging in financial transactions on unsecured public networks may result in data theft.
- **Download apps from official stores only:** This prevents the download of hazardous or deceptive software. Remain vigilant against phishing attempts: Individuals must take vigilance while replying to emails or messages that solicit personal information immediately.
- **Monitor account activity:** Fraud can be detected promptly by consistently examining your account statements.
- **Report fraud immediately:** To halt your accounts and mitigate financial damage, promptly call your bank upon seeing any irregularities.

2. MOBILE BANKING ADOPTION IN INDIA

In recent years, mobile banking and the Unified Payments Interface (UPI) have gained significant popularity in India. The swift embrace of digital payments by consumers is evidenced by the 45 billion UPI transactions recorded in 2023 alone. Nonetheless, almost 85% of e-banking app users fall between the 27 to 37 age demographic.

Nonetheless, prior to utilizing digital financial services, elderly persons necessitate additional time, reassurance, and confidence. The swift progression of technology often poses challenges for them. Research indicates that older persons are generally less proficient with technology and often lack the confidence to utilize new applications and digital platforms.

The limited utilization of mobile banking among older persons, as indicated by studies, serves as solid evidence of the digital divide. In India, 54% of the population possesses a smartphone, however hardly 5% of these users are aged over 55. This demonstrates the magnitude of the discrepancy.

TYPES OF TRANSACTIONS AVAILABLE IN MOBILE BANKING

Mobile banking has transformed our financial management practices. We can settle our bills, transfer funds, verify our account balances, and even acquire stocks with a few taps on our mobile devices. Individuals appreciate mobile banking for its flexibility and user-friendliness. The capacity to do various business transactions while traveling is one of the most advantageous aspects of mobile banking. This section will address the many sorts of transactions facilitated by mobile banking.

Account Management Transactions: The most basic functions achievable through mobile banking are account management transactions. Users can modify their personal information, access their account balances, and retrieve a comprehensive list of all transactions.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

These transactions are crucial for overseeing your funds and guaranteeing the accuracy of the data in your account. You can also receive reminders when monies are deposited or when your account balance decreases.

Fund Transfer Transactions: Funds can be transferred between accounts both within and outside your bank through fund transfer transactions. Funds can be transferred to other individuals' accounts or utilized for purchases at retail establishments. Most mobile banking applications enable users to transfer funds either periodically, on a predetermined schedule, or instantaneously. To conserve time and prevent the oversight of payments, you may establish automatic transfers.

Bill Payment Transactions: Utilizing bill payment transactions, you can promptly settle your invoices via your mobile banking application. Payments for credit card bills, loans, utilities, and other obligations can be made. Most mobile banking systems allow for online bill payments. Payments can be scheduled in advance, automated, and accompanied by reminders for upcoming due dates. To ascertain the success of your payment, you may also examine your payment history.

Mobile Check Deposit Transactions: Mobile check deposit operations enable the deposit of checks via your mobile device. The app allows you to capture images of both the front and back of the check and transmit them to your bank via email. Mobile check deposits are efficient and expedient as they eliminate the necessity of visiting a bank or ATM. Nonetheless, some banks may impose limitations on the number of monthly deposits and the amount of money that can be deposited.

Investment Transactions: You can acquire stocks, mutual funds, and other assets using your mobile banking application through investment transactions. You may acquire and divest equities, observe market conditions, and assess your investing portfolio. Most mobile investment applications have research functionalities, real-time quotation updates, and price fluctuation notifications. One must be knowledgeable in investing and have substantial experience to execute investment transactions. Consequently, it is imperative to undertake independent research and consult with specialists.

3. LITERATURE SURVEY

Sharma, S., & Joshi, A. (2020): This empirical research assesses the cybersecurity awareness of Indian bank clients and its impact on their online safety practices. The 850-person poll indicates significant disparities in cybersecurity competence across individuals in rural and urban locations. The majority of consumers possess inadequate understanding regarding online safety, the permissions required by mobile applications, and methods for securing their passwords. The authors identify a substantial correlation between the adoption of secure mobile banking practices and prior knowledge about cybersecurity. The research highlights the influence of income, education, and age on individuals' comprehension of digital security. Sethi, R., & Singh, M. (2021): This research examines the increasing prevalence of phishing attacks aimed at

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

Indian banking organizations and their clientele. The writers employ diverse case studies and papers from 2018 to 2021 to categorize phishing strategies, encompassing email scams, counterfeit banking websites, and deceptive SMS notifications. The analysis indicates that ignorance and insufficient detection procedures are the principal causes of these attacks. Statistics indicate that phishing attempts surged by more than 40% subsequent to the pandemic and the transition to digital platforms. The authors emphasize the necessity of implementing two-factor authentication and maintaining continuous surveillance to avert assaults.

Gupta, M. (2022): Gupta's research offers a comprehensive analysis of the transformative impact of mobile banking on India's financial environment, highlighting its critical role in promoting financial inclusion for underbanked and unbanked populations. This publication compiles the findings of several studies and policy frameworks, including the Pradhan Mantri Jan Dhan Yojana and the Digital India program. It addresses the limited utilization of digital banking services by consumers due to uncertainty and security concerns. The author underscores that while technology has enhanced banking accessibility, numerous people remain susceptible to scams due to inadequate understanding of cybersecurity.

Orucho, D. O. (2023): This article examines the technological facets of data security in mobile banking, including the hazards associated with data transmission between users and banking systems. It analyzes the deficiencies in the network settings, tokenization methods, and encryption protocols employed by prominent banking applications. The research employs traffic monitoring and penetration testing to identify security vulnerabilities that hackers may exploit for unauthorized access. Studies demonstrate that obsolete encryption methods and defective APIs are significant contributors to data breaches. The author asserts that, despite users' perceptions of safety, numerous mobile banking applications fail to consistently upgrade their security protocols.

Singh, R., & Kumar, V. (2024): This report analyzes the operational, legal, and regulatory challenges confronting Indian mobile banking. It illustrates the insufficiency of the current rules pertaining to cybercrime, data protection, and adherence to regulations for online financial transactions. The authors examine various case studies, including data breaches and customer grievances, to illustrate the impact of ambiguous legislation on both banks and consumers. The research analyzes the prospective modifications to mobile banking legislation resulting from the new Data Protection Bill. The paper delineates difficulties such as cross-jurisdictional data transfer and customer liability in criminal actions, based on interviews with financial and legal specialists.

Afzal, M. (2025): This research explores the relationship between cybersecurity skills and digital financial inclusion within India's rapidly growing fintech sector. It underscores that consumers, especially in rural and semi-urban regions, will experience enhanced security if they are more knowledgeable about password management, online safety, and the prevention of digital theft. The research, utilizing survey data from 1,200 participants, demonstrates that

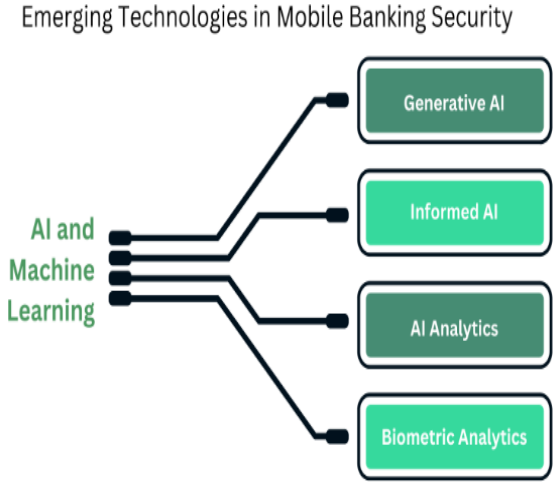
International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

cybersecurity awareness significantly influences confidence in digital financial services and the utilization of mobile banking.

Soni, A., & Sharma, P. (2025): This analytical research examines the various security issues that threaten the integrity of India's mobile banking systems. It addresses social engineering threats such as phishing and counterfeit applications, together with technological challenges such malware infections, unauthorized access, and SIM-swapping attacks. The research utilized many methodologies, including expert interviews and user surveys, to assess Indian perceptions and responses to risk. Research indicates that many consumers lack awareness of essential cybersecurity measures, such as password protection and application verification.

4. RELATED WORK

EMERGING TECHNOLOGIES IN MOBILE BANKING SECURITY



Generative AI: Generative AI is essential in mobile banking security as it creates hypothetical attacker scenarios, enabling systems to foresee and prepare for such attacks. It can generate genuine malware or phishing campaigns that instruct AI systems to identify fraud. This proactive approach improves threat intelligence and aids institutions in detecting vulnerabilities prior to potential exploitation by attackers. It is additionally employed to enhance the security of systems that encrypt data and authenticate identities.

Informed AI: Incorporating machine and human intelligence, informed AI utilizes data to enhance security decisions. It examines general human behavior and the completion of transactions to identify anomalous activities in real time. This technology enables mobile banking systems to authenticate the accuracy and utility of messages through verification by both humans and machines. It safeguards items without modifying the user's interaction with them.

AI Analytics: AI analytics refers to the process of scrutinizing extensive banking data for signs of fraud, anomalous activity, and security vulnerabilities. Utilizing anomaly detection and predictive modeling, it can identify risks more rapidly than earlier systems. Financial institutions, including banks, utilize AI analytics to autonomously monitor transactions and detect anomalies. This guarantees the security of online monetary transactions and the integrity of mobile banking networks.

Biometric Analytics: Biometric analytics enhances mobile banking security by verifying a user's identity through the analysis of behavioral or physical traits, like speech patterns, facial recognition, and fingerprints. Individuals become less dependent on readily compromised passwords and PINs, hence diminishing the probability of unauthorized access. Sophisticated biometric algorithms analyze

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

patterns to detect fraudulent attempts or aberrations. This technology is exceptionally intuitive and secure.

SECURITY CHALLENGES AND RISKS OF MOBILE BANKING

Mobile banking presents several challenges that require resolution. It is essential to comprehend these hazards, their mechanisms, and the methods to avoid them.

Key security challenges and risks in mobile banking are:

- Phishing attacks
- Weaknesses in traditional authentication methods and systems
- Device theft and unauthorized access
- Man-in-the-middle attacks

Phishing Attacks

Phishing is a prevalent form of fraud. These attacks manipulate victims into revealing personal account information, such as passwords, usernames, and two-factor authentication details. Phishing attempts sometimes manifest as fraudulent emails, SMS messages, websites, and alerts. To acquire individuals' login passwords, certain skilled hackers may develop counterfeit banking applications.

Weaknesses in Traditional Authentication Methods and Systems

Cybercriminals exploit vulnerabilities in the authentication techniques often employed by mobile applications. Weak passwords, incorrect configuration of multifactor authentication (MFA), and the reuse of login credentials across several platforms might facilitate unauthorized access to individuals' mobile banking accounts.

Device Theft and Unauthorized Access

Cell phones and other portable devices are susceptible to theft or loss, granting access to sensitive information, including bank accounts. Financial institutions utilize biometric verification, personal identification numbers, and passwords; yet, cybercriminals possess the expertise to bypass these security measures.

Man-in-the-middle Attacks

A man-in-the-middle (MitM) attack transpires when an unauthorized entity interferes with the communication between a user and the banking server. An assailant may, for instance, acquire a user's login credentials over an unsecured network or public Wi-Fi, or they may obtain a one-time password through a precarious means.

5. ANALYSIS AND DISCUSSION

TABLE 1 — ANNUAL SECURITY PROGRAM: BUDGET VS ACTUAL SPEND

Year	Budget	Actual Spend	Variance
FY2020-21	5	4.5	-0.5
FY2021-22	8	9	1
FY2022-23	12	11	-1
FY2023-24	15	14.2	-0.8
FY2024-25	18	17.5	-0.5
Total	58	56.2	-1.8

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

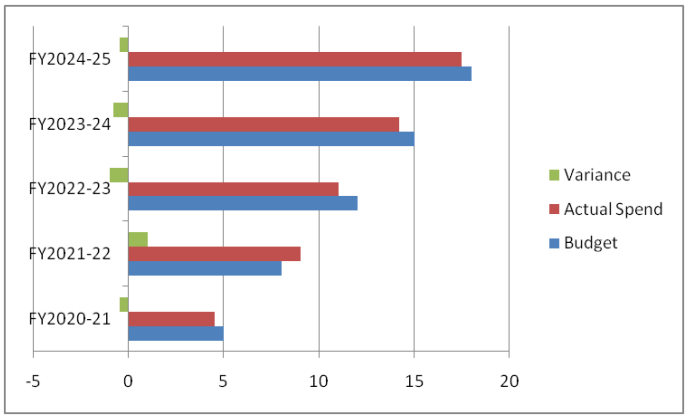


TABLE 2 — TRAINING COSTS BREAKDOWN

Year	Content Dev	Trainers	Travel & Venue	Digital Modules	Other	Total
FY2020-21	0.8	0.6	0.2	1	0.1	2.7
FY2021-22	1	0.8	0.3	1.5	0.2	3.8
FY2022-23	1.5	1	0.4	2	0.3	5.2
FY2023-24	1.8	1.2	0.5	2.8	0.4	6.7
FY2024-25	2	1.5	0.6	3.5	0.5	8.1
Total	7.1	5.1	2	10.8	1.5	26.5

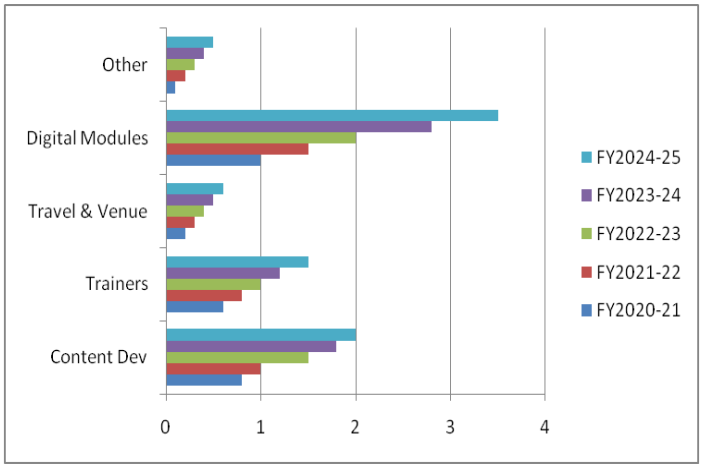


TABLE 3 — FRAUD: DETECTED Vs PREVENTED Vs NET LOSS

Year	Detected Fraud	Prevented Fraud	Net Loss (Detected − Prevented)
FY2020-21	25	10	15
FY2021-22	30	14	16
FY2022-23	40	22	18
FY2023-24	35	25	10
FY2024-25	28	24	4
Total	158	95	63

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

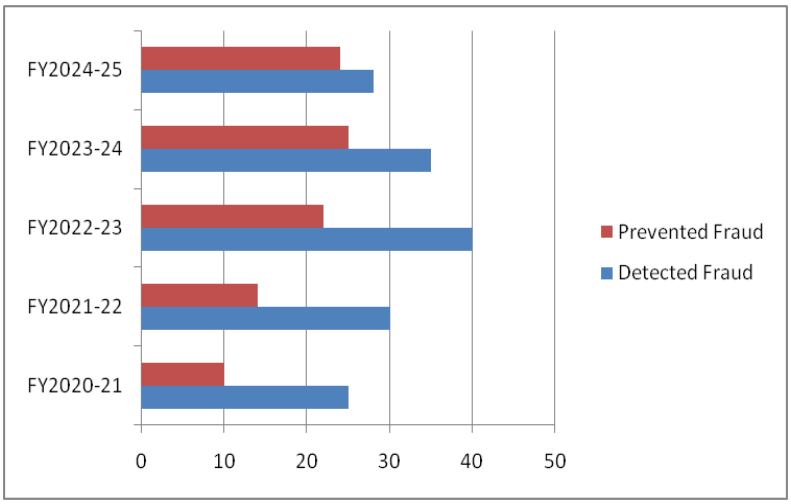


TABLE 4 — ANNUAL ROI ON SECURITY INVESTMENTS

Year	Investment (Actual Spend)	Estimated Annual Savings	ROI (%)
FY2020-21	4.5	8	177.78%
FY2021-22	9	10	111.11%
FY2022-23	11	14	127.27%
FY2023-24	14.2	20	140.85%
FY2024-25	17.5	26	148.57%
Cumulative	56.2	78	138.79%

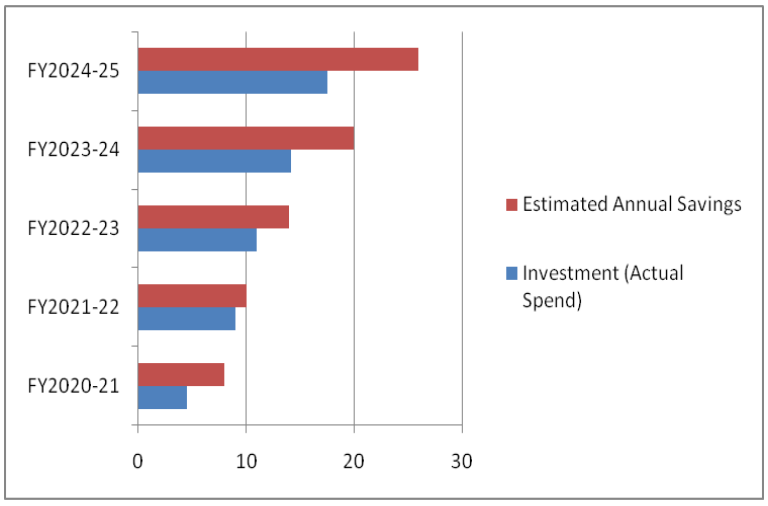


TABLE 5 — MOBILE CHANNEL REVENUE & COST SAVINGS

Year	Active Mobile Users (mn)	Mobile Revenue	Cost Savings (fraud + automation)
FY2020-21	5	120	15
FY2021-22	6.2	180	22
FY2022-23	8	260	30
FY2023-24	10.5	380	45
FY2024-25	13	520	68

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

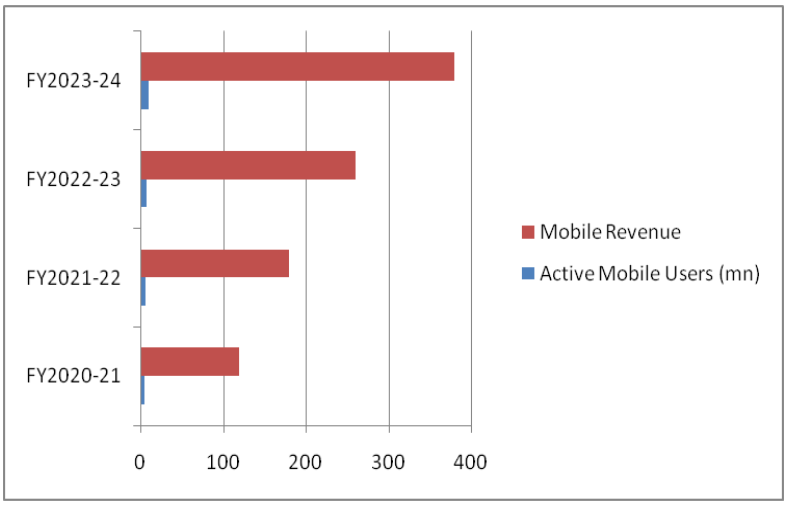
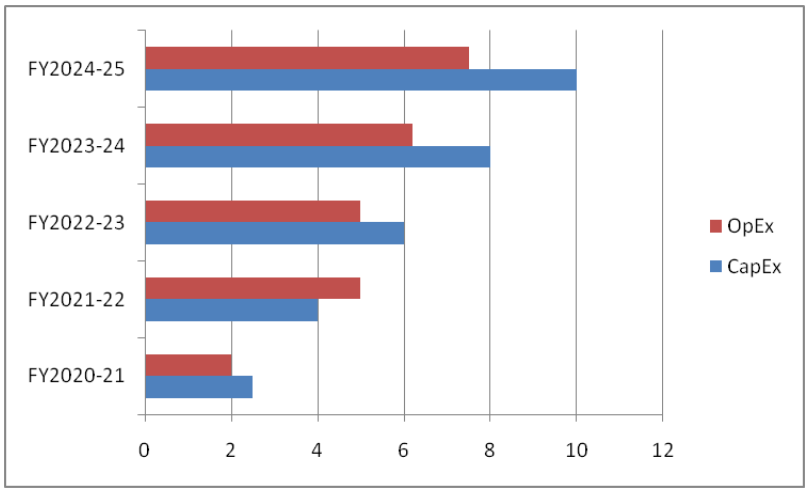


TABLE 6— TECHNOLOGY INVESTMENT SPLIT (CAPEX VS OPEX)

Year	CapEx	OpEx	Actual Spend (CapEx+OpEx)
FY2020-21	2.5	2	4.5
FY2021-22	4	5	9
FY2022-23	6	5	11
FY2023-24	8	6.2	14.2
FY2024-25	10	7.5	17.5
Total	30.5	25.7	56.2



DISCUSSIONS:

Annual Security Program: Budget vs Actual Spend

Actual expenditure stayed mostly aligned with the budget, exhibiting only minor variations over years. The budget was effectively managed owing to a total underspending of ₹1.8 crore. Certain programs may be eligible for expansion if they were underutilized in previous years.

Training Costs Breakdown

Expenditure on training has increased, with a significant portion allocated to the creation of online tools and curriculum. This redesign aims to implement more contemporary and user-friendly training

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

approaches. The increased total cost indicates that employees are more dedicated to gaining new skills and enhancing their existing ones.

Fraud: Detected vs Prevented vs Net Loss

Although fraud detection initially improved, numerous precautions were implemented to prevent it by FY2024–2025. Due to the effectiveness of the fraud prevention techniques, the net loss decreased from fifteen to four. This development indicates an enhancement in security and monitoring protocols.

Annual ROI on Security Investments

The return on investment (ROI) for security expenditures reached a zenith of 177.78% in fiscal year 2020-21, sustaining its strength subsequently. The company demonstrates strong financial performance with a return on investment of approximately 139%, effectively mitigating losses. It is wise to persist in security investments, according to these statistics.

Mobile Channel Revenue & Cost Savings

A significant segment of mobile phone revenue and user base experienced rapid growth year-over-year. Income increased by over fourfold within five years. The automation of procedures and the prevention of fraud enhanced operational efficiency, resulting in reduced expenses. The research's findings indicate significant cost reductions and revenue generation via the mobile platform.

Technology Investment Split (CapEx vs OpEx)

A comprehensive investment plan in technology is evidenced by the increase in both capital and operational expenditures. With the increased emphasis on capital expenditures (CapEx), expenditures on development and infrastructure also escalated. As real investment increases consistently, so do the objectives of digital transformation.

6. CONCLUSION

Finally, by enhancing convenience, speed, and accessibility, mobile banking has fundamentally revolutionized financial management in India. As reliance on digital platforms increases, the likelihood of individuals becoming victims of cybercrime, data breaches, and fraud also escalates. Human vigilance, including the avoidance of phishing, utilization of secure networks, and monitoring of account activity, is equally crucial as technological safeguards, such as robust passwords, two-factor authentication, regular updates, and dependable security software, in the context of mobile banking. Equally crucial is educating individuals on the safe utilization of their gadgets and the appropriate actions to take in the event of an emergency. By prioritizing technical steps and ongoing education, individuals can significantly reduce the risk of financial loss, enhance confidence in online banking systems, and contribute to the security of India's mobile banking ecosystem.

REFERENCES

1. Afzal, M. (2025). Cybersecurity awareness and digital financial inclusion in India’s fintech ecosystem. Journal of Digital Finance & Cybersecurity, 14(1), 19–41.
2. Gupta, M. (2022). Mobile banking and financial inclusion in India: A review of accessibility, trust, and

ISSN: 3107-7900, P.CODE: 26/2-1/08
DOI: https://doi.org/10.5281/zenodo.18910412

cybersecurity. International Review of Digital Banking & Inclusion, 9(3), 27–49.

3. Mungara, D. (2025). Security and privacy recommendations for UPI users: A behavioral and technical assessment. UPI Security & Digital Payments Review, 11(2), 33–56.
4. Orucho, D. O. (2023). Data transmission vulnerabilities in mobile banking applications: A technical security analysis. Journal of Mobile Banking Security & Encryption, 7(1), 22–45.
5. Sethi, R., & Singh, M. (2021). Phishing attacks on Indian banking customers: Trends, techniques, and preventive measures. Cybercrime & Banking Security Journal, 6(2), 31–54.
6. Sharma, S., & Joshi, A. (2020). Cybersecurity awareness among Indian banking customers: Impacts on online safety behavior. Journal of Cyber Awareness & Financial Safety, 5(1), 15–37.
7. Singh, R., & Kumar, V. (2024). Legal, regulatory, and operational challenges in India's mobile banking ecosystem. Digital Banking Law & Compliance Review, 8(3), 41–63.
8. Soni, A., & Sharma, P. (2025). Security risks in mobile banking systems: Technical vulnerabilities and behavioral factors. Mobile Banking Risk & Protection Journal, 12(2), 26–48.
9. Srinivasan, R., & Reddy, P. (2025). User perceptions of security and privacy features in mobile banking applications. Journal of Mobile App Security & User Behavior, 13(1), 17–39.
10. Tiwari, S., & Singh, R. (2025). Awareness of app-based mobile banking services: Safety, usability, and digital literacy. Mobile Banking Literacy & Safety Review, 10(2), 44–66.
11. Vijayakumar, S., & Ramesh, S. (2025). Cybersecurity challenges faced by senior citizens in mobile banking adoption. Journal of Senior Digital Safety & Financial Inclusion, 9(1), 23–46.
12. Yadav, S., & Singh, A. (2025). Cybersecurity threats in India's BFSI sector: A comprehensive digital threat assessment. BFSI Cyber Threats & Risk Intelligence Report, 15(1), 51–78.