ज्ञानविविधा
कला, मानविकी और सामाजिक विज्ञान की सहकर्मी-समीक्षित, मूल्यांकित, त्रैमासिक शोध पत्रिका

ISSN : 3048-4537(Online)
3049-2327(Print)
IIFS Impact Factor-6.125
Vol.-3; Issue-2 (Apr.-June) 2026
Page No.- 301-307
DOI :-10.71037/gyanvividha.v3i2.45

https://journal.gyanvividha.com

Author's :
1. PANKAJ KUMAR CHOUDHARY JAT
Research Scholar.
2. Dr. Sandeep Kumar Chaurasia
Supervisor, Assistant Professor, School of Management Studies, Sangam University, Bhilwara.

Corresponding Author :
PANKAJ KUMAR CHOUDHARY JAT
Research Scholar.

Security, Trust and Risk Perception in Digital Banking : A Study of Private Sector Bank Customers in Ajmer Division

Abstract : Digital banking has revolutionized the way we conduct banking services with speed, low cost, and convenience. However, as the number of digital banking customers has increased, so has the number of complaints related to privacy, fraud, transaction failures, and poor handling of complaints. This paper studies the influence of security, trust, and the perception of risk on the digital banking behavior of customers of private sector banks in Ajmer Division. It analyzes published peer-reviewed research, banking reports, and evidence on cybersecurity and other Rajasthan-specific published materials from 2021 to 2026. No primary data has been surveyed. It has been found that the perception of risk, trust, and convenience has the most influence on the discontinuation of the use of digital banking. Data fraud, phishing, identity theft, and trust eroding incidents of cybercrime have the most negative influence on trust. Clear messaging, easy to use systems, visible security, fast complaint resolution, and branch support positively influence trust. Convenience and speed of digital banking channels have influenced their adoption. Evidence from other parts of the country shows that an increase in digital banking is directly related to an increase in complaints. The complaints from Rajasthan, especially Ajmer's involvement in a fraud project, indicates the concern of the complaints. The paper also argues that private banks should consider customer protection to be part of a high quality service offering and not an IT function.

Keywords: Digital banking; cybersecurity; trust; perceived risk; private sector banks; Ajmer Division; customer protection.

1. Introduction : Digital banking covers a wide range of activities, including mobile application banking, internet

banking, banking through UPI, banking by using cards, banking by way of electronic transfers, and banking through requests for services offered by applications. Digital banking helps save the time and effort that would otherwise go to travelling to and waiting at the bank. It makes banking available to customers even after banking hours. All of these advancements are useful for the various customers of banks in the Ajmer Division, involving urban banking centers, small towns, and all the different categories of customers from traders and salaried employees to students, pensioners, and the rural population.

Despite the various problems and challenges associated with digitization, India's digital payments jumped by 276 percent in a short time from 4,370.68 crore transactions in 2020-21 to 16,443.02 crore transactions in 2023-24. In the ongoing financial year, by January 2025, over 18,120.82 crore transactions were estimated to have taken place. Along with this, device binding, two-step verification, transaction ceilings, and AI-based fraud alerts were also institutionalized (Ministry of Finance, 2025). However, as with any system, the growth of an organization exposes it to various risks. Digital banking can very quickly cause a financial loss to a customer if that customer follows a fraudulent KYC link, shares their OTP, installs a remote-control access app, or calls a fake customer care number.

The primary issue is not how to get customers to adopt banking systems, but how to adopt these banking systems in a manner that is safe and has a sustained impact. From a banking system's point of view, security refers to the systems and controls in place to safeguard bank accounts, devices, data, and the integrity of each banking transaction. Trust, from a customer's standpoint, is the belief that the bank has the necessary skills and integrity to provide services and assist the customer in a timely manner in the event that something goes wrong. Perceived risk, from a customer's standpoint, is the expectation of the customer of a financial loss, a loss of privacy, an interruption of service, or psychological stress. These are all interrelated and are closely linked.

Private sector banks deserve close attention since they use digital services, application design, personalized offers, and low-contact services to compete. Although these may enhance customer satisfaction, they may also transfer more burden to the customer. This paper will focus on the following questions: How do security perceptions influence trust? What kind of risks prompt customers to stop using a service? What do the customers of the Ajmer Division consider the most protective measures? The paper will use the most recent studies and published data to provide answers. It will not report the results of an original household survey for Ajmer.

2. Review of Literature : New evidence from Indian researchers indicates that usefulness alone cannot justify digital banking behavior. Kumar et al. analyzed 253 young users of mobile banking. They reported that along with trust, the following elements were important for the intention to adopt and use mobile banking: performance and effort expectancy and social and financial costs. Perceived risk served to counteract trust and the intention to use banking in practice (Kumar et al., 2023). Tiwari, Tiwari, and Gupta found that in the Indian context of mobile banking, trust, risk, and the other basic elements of the acceptance of a new technology should also be considered (Tiwari et al., 2021). The above studies suggest a consistent framework. Consumers might perceive the digital service positively, but that will not translate into habitual use unless the perceived service is devoid of uncertainty.

Trust also acts as a bridge. Chawla et al. studied digital natives in 5 Indian cities. They reported that perceived trust, perceived security, and perceived risk were also important for the adoption of financial technologies, and trust was part of the relationship of the above three perceived elements (Chawla et al., 2023). Gupta, Wajid, and Gaur also reported that perceived

trust and perceived benefits had positive relationships to the intention to continue to use FinTech in India, whereas perceived risk had a negative relationship (Gupta et al., 2024). Jangir et al. showed that risk was a determinant of continuance behavior, not acceptance behavior (Jangir et al., 2023). Therefore, a user might download a banking application because of its usefulness, but might stop using the application because of a suspicious transaction or an upsetting notification.

Age and confidence are very much important. Jena's analysis of 456 senior citizens in central India revealed that trust, perceived risk, anxiety, self-efficacy, usefulness, and ease of use are significant predictors of e-banking intention (Jena, 2023). This relates to Ajmer's pensioners and senior account holders. A process designed with technical security may still be perceived as unsafe when the instructions are complicated. Accessibility and the acceptance of technology are also related to online banking use in post-Covid India (Lee et al., 2025). Security must be both effective and understandable.

Recent literature focuses on the experiences of cybercrime and the redress of related grievances. Perceived usefulness, ease of use, and social impact, in addition to the improvement of trust and the perception of cybersecurity as a grievance, were found to be influenced by prior cybercrime experience and the improvement of trust and perception of cybersecurity among 650 Indian users (Aljaradat and Shukla, 2025). The latter study of 732 active users in North India found a positive relationship of ease of use, performance expectancy, and grievance redress to use. Perceived cybersecurity risk had a strong negative relationship with trust. In this study, trust did not, and use directly, predict trust, but it did, and support, performance expectations (Aljaradat and Shukla, 2026). This is a significant improvement. Trust may act in an indirect manner.

Outside India, the same reasoning applies. Among 1,133 small businesses in Indonesia, continued mobile payment usage was impacted by a trust-related risk, and the perceived benefits were insufficient to mitigate the associated fear (Nugroho and Paramita, 2024). Additionally, the evolution of digital risk and financial inclusion indicates that, without protection for users, the innovations can potentially marginalize the users it intended to serve (Ahmed et al., 2024). Also, through game-theoretic work, it has been postulated that users, banks, and attackers continuously adjust to one another. Thus, security is a repeated strategic process and not a one-time aspect (Aljaradat et al., 2024). In this context, the literature endorses risk-sensitive and customer-centric banking.

3. Research Methodology : This study uses a descriptive and analytical framework for secondary research. It focuses on private sector bank customers in the Ajmer Division; however, recent bank-specific microdata for Ajmer are not available to the author, necessitating a wider research base. This study makes a regional analysis and does not cite national data as local survey data.

Eighteen sources were chosen. They are peer-reviewed journal articles, the Ombudsman report of the Reserve Bank of India, a report of the Parliamentary Standing Committee, Ministry of Finance payment data, a national threat report on the banking sector, and an operational note pertaining to the state of Rajasthan. The majority of the sources were published between 2021 and 2026. Sources were selected if they mentioned digital banking or were relevant to the subjects of payments, security, trust, perceived risk, cybercrime, accessibility, or the grievance redress process. Descriptive news pieces and unverifiable commercial statements were excluded.
There were three stages to the analysis. The first stage involved the extraction of quantitative indicators within the context of the growth of banking transactions, cybercrime complaints, complaints to the Ombudsman, shares of complaints, sample sizes, and the results of various

models. The second stage involved coding the literature. The final stage involved the contextualization of the coded literature with specific emphasis on the older segments of the user population, small traders, the banking poor, and those users who required branch services.

The results are a formal synthesis of evidence. Likely trends and operational hazards are demonstrated. The studies are unable to measure the exact percentage of Ajmer Customers who trust or distrust a private bank. The next primary research study should implement stratified sampling in urban, semi-urban and rural areas, along with separate analysis in the factors of age, education, income, bank, and prior fraud experience.

4. Security, Trust and Risk in Ajmer Digital Banking : For users of the Ajmer Division, the integration of digital security is perceived in everyday moments. It is when their login succeeds, OTPs arrive, fund transfers get processed, and complaints get addressed by a real person. These build and sustain trust. This trust can be swiftly eroded. It is when a service application is unsuccessful, money is deducted with no status, and the customer is shuttled between a chatbot, call center, and branch.

The local issue is concrete. Based on secondary evidence, a strategy note by CUTS and Dvara Research has listed Ajmer among other Rajasthan districts that have been selected owing to relatively high cyber-fraud occurrences. The note suggested that researchers study poor women, farmers, poor women farmers, low-income families, micro-enterprises, merchants, e-Mitra service providers, and business correspondents (CUTS and Dvara Research, 2022). This does not confirm the absence of all division fraud cases. It illustrates the need for customer-level research.

There are three important types of trust. One is technical trust, and this can be instilled through secure authentication, encryption, binding to devices, and anomaly detection. Another is institutional trust, and this can be created through the bank having a good reputation, clear rules for liability, and a just resolution of complaints. The last is experiential trust, and this is the trust that the customer or the customer's family has gained through their personal experiences. This can be the most powerful of the three. A person who has lost money may remain distrustful even after the bank provides a secure explained system (Aljaradat and Shukla, 2025).

Risk is also multidimensional. Financial risk means direct monetary loss. Privacy risk involves the account, identification, and location, and contact data being abused. Performance risk arises from a transaction that has not been executed, or that has been delayed. Social risk occurs when family members criticize the user for the loss. There is time risk and this is caused from long waits and multiple visits to the branch to file a complaint. Psychological risk is the anxiety, shame, and fear caused by the event. This is exacerbated for the older customers (Jena, 2023).

The risk landscape is rapidly changing. The national BFSI threat report identifies real-time fraud, insecure application interfaces, phishing, malware, credential theft, supply-chain vulnerabilities, and social engineering attacks augmented by AI as threats of concern. Layered security, real-time threat intelligence, improved authentication standards, application security, and anomaly detection are all recommended (CERT-In et al., 2025). However, controls for the end user should be less complex. Too many alerts can result in warning fatigue.

Private banks in Ajmer should implement technology with local support. Helpful measures can be Hindi alerts in simple language, digitally assisted onboarding by the branch, a verified callback support, a clearly visible freeze transaction option, additional checks for atypical transfers, and support with priority response for the elderly. The RBI's fraud awareness report also highlights the need to instantly report any fraud, as delays directly correlate with an

increase in the perpetrated fraud (Reserve Bank of India, 2024). Security communication should instruct users to take an action instead of prohibiting an inaction.

5. Data Analysis and Results : Secondary data indicate four major trends for digital banking adoption, customer complaints, cybercrime, and trust in digital financial systems. First, the adoption of digital payments in India has been astonishing. The Ministry of Finance (2025) reports that the number of digital transactions in India increased by approximately 276% from the financial year 2020–21 to the financial year 2023–24. With this overwhelming growth, India stands as a case example of the increasing reliance on technology and digital banking. While this may be attributed to the success of the Indian government's campaign for financial inclusion, the stark increase in digital payments exposes the Indian banking community to the threat of cybercrime, illicit social engineering, and dispute transactions.

Second, there has also been an overwhelming increase in customer complaints regarding banking services. The RBI Integrated Ombudsman reports that the number of customer complaints lodged in the 2023–24 period reached 934,355, which is 32.81% higher than the previous year. Of this, 57,242 complaints related to mobile and online banking. Private sector banks accounted for the most complaints of all the regulated entities, and the state of Rajasthan was one of the states with the highest number of complaints of banking services for every lakh of deposit and credit accounts (Reserve Bank of India, 2025).

Third, evidence of cybercrimes presents new challenges of increased financial vulnerability. The Parliamentary Standing Committee stated that cybercrimes increased from 9.7 lakh in 2022 to 11.5 lakh in 2023, with almost 60 percent reporting financial fraud. The financial loss reported increased from ₹ 2,296 crore in 2022 to ₹ 5,574 crore during the period of January to October, 2023. The recovery and restoration rates of lost finances continued to remain low, with 10.4 percent of the lost finances restored in the period of 2021-2022 (Standing Committee, 2024). All these trends only add to the perception of risk and loss of trust in digital transactions.

Fourth, the behavioral studies cited, as part of this report, emphasize the central idea of trust in the continued use of digital payments. The trust and the use of a system are impacted by the ease of use and the perception of the system's security. The experience of cybercrimes is shown to negatively impact the trust and the continued use of the system (Aljaradat & Shukla, 2025; 2026). The studies cited, show that the user experience is a system of trust and that the continued use of the system is also an experience of trust and the user is a partner in the system. Failure to communicate and negative user experiences result in a return to traditional banking services. Therefore, the trust of the user is strengthened by a system that is designed to prevent fraud, ease of use, real-time communication, and resolution of user complaints.

6. Discussion : The results show that trusting digital banking is not a fixed attitude among customers but is an evolving behavioral outcome that can be built with multiple exposures to the banking platform. Although private sector banks focus on speed and convenience and offer rewards, these cannot be the sole mechanisms to ensure customers use the services for the long-term. Previous research shows that perceived risks of cybersecurity disrupt customers' transition from the adoption stage to the usage stage of digital financial services, and as a result, customers develop low loyalty to digital financial services (Jangir et al., 2023; Nugroho & Paramita, 2024). Thus, among the variables, trust is the strongest variable that connects customer satisfaction and continuous digital engagement.

This is particularly important for Ajmer, where all digital banking users are from multiple demographics and occupations. These include students, shopkeepers, pensioners, workers of the service sector, farmers, and first-time digital users, and they experience different risks and have

different levels of digital literacy. What may be a security feature that provides a user some comfort, may in fact create uncertainty in a digital banking novice. Thus, different user groups should have different awareness campaigns. For example, senior citizens may be offered training with support, while shopkeepers may be educated to protect against QR code fraud, fake payment screenshot fraud, and business account fraud. Reminders of safe digital practices may be warranted for high-risk transactions for less frequent users.

The results demonstrate that grievance redressal systems play an important role in building trust. While prevention of fraud is critical, the rapid and open resolution of complaints is also vital. Data from the RBI show a rapid increase in complaints alongside a greater reliance on digital grievance methods (Reserve Bank of India, 2025). Banks need to offer an integrated complaint mechanism at the level of their applications, websites, SMS services and branch offices. Customers should be provided a tracking number, an estimated time for resolution, and a complaint escalation procedure. Increased visibility of the National Cyber Crime Helpline 1930 can also help assist customers to a greater extent.

The creation of trust in the future should combine the detection of fraud through the Ajmer based systems with AI and the judgment of humans. The use of different languages for warning messages, combined with verification calls, can also facilitate trust along with the teaching of basic personal digital security on a semiannual basis to the users of the system. Even though this study relies heavily on data that are not primary and has no direct measurement of trust or fraud in Ajmer, it gives sufficient evidence to build the basis for future studies and the creation of policies.

7. Conclusion : There is real value in digital banking within the Ajmer Division of Rajasthan. Digital banking makes daily banking fast and convenient. The future of digital banking in the Ajmer Division relies on more than just the total number of users of the banking application or users making digital transactions. Users of digital banking in the Ajmer Division need to feel that the digital banking system is secure and that if there is a concern or issue that the bank will respond in a fair and just manner and in a timely manner.

The evidence that was evaluated consistently pointed to the same conclusion. The perception of usefulness and ease increased adoption. Trust made the system of digital banking more robust and secure. The risk of loss from finances or privacy, failed transactions, difficult interface and even past experiences of cybercrimes increase the perception of risk. These impacts are more significant to people who have lower confidence in digital banking, especially older users. The evaluation of the complaints and transaction data from the national level shed light on the urgency of the issue. The complaints from Rajasthan and identifying Ajmer as the focus of complaints add local relevance (Reserve Bank of India, 2025; CUTS and Dvara Research, 2022).

Trust-based security systems should be implemented by the private sector banks. This would include layered security, real-time detection of system anomalies with the option of user controlled instant blocking of all transactions, simple warnings in the Hindi language, and verified callbacks. This would also include the freezing of transactions, on demand, coupled with tracking of the grievance redressal system. It would also require the fair treatment of customers by bank employees. When a customer is the victim of cybercrime, bank employees should take immediate action to resolve the reported crime and provide guidance. Customers should not be blamed or referred to other employees.

This paper does not assert original survey results. Its contribution is a checked regional synthesis and a clear pathway for future research. An upcoming study on Ajmer should gather primary data from varying groups, differentiated by age, income, education, and settlement, as

well as data on customers with and without fraud experiences and the outcome of complaints that were actually filed. This kind of research would aid the private banking sector in gradually moving away from focus of only digital expansion toward creating secure digital inclusion.

References:

1. Ahmed, Faraz, et al. "Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers." *Risks*, vol. 12, no. 8, 2024, article 133.
2. Aljaradat, Aya, Gargi Sarkar, and Sandeep K. Shukla. "Modelling Cybersecurity Impacts on Digital Payment Adoption: A Game Theoretic Approach." *Journal of Economic Criminology*, vol. 5, 2024, article 100089.
3. Aljaradat, Aya, and Sandeep K. Shukla. "Cybersecurity and Trust Formation in Digital Payment Use Behaviour in North India." *Discover Sustainability*, vol. 7, 2026, article 498.
4. Aljaradat, Aya, and Sandeep K. Shukla. "Trust and Cybersecurity in Digital Payment Adoption: Socioeconomic Insights from India." *Journal of Business and Socio-economic Development*, vol. 5, no. 4, 2025, pp. 372–386.
5. CERT-In, CSIRT-Fin, and SISA. *Digital Threat Report 2024: For the Banking, Financial Services and Insurance Sector*. SISA, 2025.
6. Chawla, Udit, et al. "The Mediating Effect of Perceived Trust in the Adoption of Cutting-Edge Financial Technology among Digital Natives in the Post-COVID-19 Era." *Economies*, vol. 11, no. 12, 2023, article 286.
7. CUTS Centre for Consumer Action Research and Training, and Dvara Research. *A Holistic Representation of Frauds and Grievance Redress in Digital Payments and Digital Credit Services in Rajasthan*. Operational Strategy Note, 2022.
8. Gupta, Kanishka, Abdul Wajid, and Dolly Gaur. "Determinants of Continuous Intention to Use FinTech Services: The Moderating Role of COVID-19." *Journal of Financial Services Marketing*, vol. 29, 2024, pp. 536–552.
9. India. Ministry of Finance. "Digital Payment Transactions Surge with over 18,000 Crore Transactions in 2024-25." *Press Information Bureau*, 11 Mar. 2025.
10. India. Parliament. Lok Sabha. Standing Committee on Communications and Information Technology. *Digital Payment and Online Security Measures for Data Protection*. 2024.
11. Jangir, Kshitiz, et al. "The Moderating Effect of Perceived Risk on Users' Continuance Intention for FinTech Services." *Journal of Risk and Financial Management*, vol. 16, no. 1, 2023, article 21.
12. Jena, Rabindra. "Factors Impacting Senior Citizens' Adoption of E-Banking Post COVID-19 Pandemic: An Empirical Study from India." *Journal of Risk and Financial Management*, vol. 16, no. 9, 2023, article 380.
13. Kumar, Rakesh, et al. "How Does Perceived Risk and Trust Affect Mobile Banking Adoption? Empirical Evidence from India." *Sustainability*, vol. 15, no. 5, 2023, article 4053.
14. Lee, Cheng-Wen, et al. "Perceived ESG, Accessibility, and Technology Acceptance: An Empirical Study of Online Banking Adoption in Post-Pandemic India." *Businesses*, vol. 5, no. 4, 2025, article 52.
15. Nugroho, Sahid Susilo, and Widya Paramita. "Trust-Building Mechanism for Promoting Mobile Payments' Continued Use by Small Businesses in a Developing Country: Tackling the Perceived Risk Issue." *Journal of Financial Services Marketing*, vol. 29, 2024, pp. 936–945.
16. Reserve Bank of India. *Annual Report of the Ombudsman Scheme, 2023-24*. Consumer Education and Protection Department, 24 Jan. 2025.
17. Reserve Bank of India. *Financial Awareness Messages*. Financial Inclusion and Development Department, 2024.
18. Tiwari, Prashant, Shiv Kant Tiwari, and Ashish Gupta. "Examining the Impact of Customers' Awareness, Risk and Trust in M-Banking Adoption." *FIIB Business Review*, vol. 10, no. 4, 2021, pp. 413–423.

•