



Digital Banking and Cyber Frauds in India: An Analytical Study with a Focus on Rural Areas

Dr. Mahesh Prasad^{a, *}, 

^a Assistant Professor (Law), Govt. Shrimant Madhavrao Scindia P.G. College, Shivpuri, Affiliated to Tatyta Tope Vishwavidyalaya, Guna (M.P.), India.

KEYWORDS

Cyber Frauds, Rural India, Digital Payments, Financial Inclusion, Banking Security, UPI Transactions, Online Banking, Rural Consumers, Digital Literacy, Cybersecurity Awareness, Digital Banking, Cybercrime.

ABSTRACT

The fast growth of digital banking in India has revolutionized the banking sector, enriching accessibility, convenience, and financial inclusion to various demographics. The technology is playing a significant role in adoption of banking services, especially in rural areas, with the government initiative and the penetration of smart phones and the usage of banking payment platforms. Conversely, the ever-growing dependence on the application of digital financial services has also witnessed a significant surge in cyber frauds, which pose severe challenges to users, financial institutions and policy makers. Rural customers are at a greater risk because they are less likely to be digitally literate or have knowledge of cybersecurity, as well as have access to technical support systems.

This study aims to analytically comprehend the digital banking revolution and the surge of cybercrimes in India particularly in rural India. The study examines how far the adoption of digital banking is and pinpoints the most prevalent types of cyber fraud affecting rural consumers and analyzes the contributing factors to make consumers vulnerable to cyber fraud. The study also examines the extent to which customers of rural banks are aware about Cyber Security and effectiveness of the existing preventive measures. With the help of the analysis, the significance of improved financial literacy training on digital banking, robust security mechanisms and collective action by banks, government and regulatory authorities to address new cyber threats to rural consumers is emphasized. The results help in understanding the link between digital financial inclusion and cybersecurity issues in rural India and suggest empirical steps to encourage secure and sustainable practices in digital banking.

1. Introduction

Digital technologies have revolutionized the banking industry, with their adoption in delivering financial services to customers. Digital banking has

become a useful and efficient way to carry out financial activities also minimizing the reliance on conventional branch-based banking. In India, the adoption of digital financial services has grown in

Corresponding author


**E-mail: rayom.com@gmail.com (Dr. Mahesh Prasad).

DOI: <https://doi.org/10.53724/lrd/v10n2.2>

Received 7th Oct. 2025; Accepted 20th Nov. 2025

Available online 30th December 2025

2456-3870/©2025 The Journal. Publisher: Welfare Universe. This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

 <https://orcid.org/0009-0008-7248-6552>



recent years due to the growing influence of the Internet, smartphones and government efforts towards digitising the nation. Digital banking has made life easier for customers however it has also been a step towards bridging the gap between banks and weaker sections of society to access banking services. With the dawn of digitisation, however, come with them risks like cyber-attacks and financial frauds, which make it harder for consumers and financial institutions (Reserve Bank Information Technology Pvt. Ltd. [ReBIT], 2018; Gateway House, 2019).

1.1 Background of the Study

No doubt, digital technologies have changed the face of the international finance sector and given customers the freedom to bank anywhere, anytime. The digital transformation of banking has gained momentum in India with several initiatives and programs such as Digital India, Pradhan Mantri Jan Dhan Yojana (PMJDY), Aadhaar integration, and Unified Payment Interface (UPI). These innovations have paved the way for seamless transactions, cost savings and financial inclusion. While these advantages have come, the rapid growth of digital financial services has also been accompanied by a number of cyber risks, such as phishing attacks, identity theft, unauthorized transactions, and social engineering scams. It is, therefore, crucial to comprehend the correlation between the expansion of digital banking and cyber fraud to safeguard the digital financial landscape and ensure its sustainability (ReBIT, 2018; Kumar, 2025).

1.2 Digital Banking Scenario in India

India has one of the world's fastest growing markets for digital payments. The banking system has been

revolutionized by the introduction of internet banking, mobile banking, digital wallets, and transactions through UPI. Government efforts to encourage cashless payments and developments by banks and fintech companies have put a spotlight on digital payments. The Reserve Bank of India (RBI) has played a pivotal role in shaping the digital financial landscape, driven by its regulatory moves and security measures. Moreover, recent initiatives such as the Unified Lending Interface (ULI) are geared towards providing access to digital financial services and credit to underserved and rural populations, thereby strengthening the country's digital financial ecosystem (ReBIT, 2018; Reuters, 2024).

1.3 Emergence of Cyber Frauds in the Digital Era

Digital banking has made financial information and transactions more accessible and efficient but also has enabled cybercriminals to take advantage of vulnerabilities in technology and people. Cyber frauds like phishing, vishing, smishing, OTP theft, QR-code scams, fake loan applications, UPI-related cyber frauds have proliferated in times gone by. Fraudsters usually focus on people who are not as knowledgeable about cybersecurity, especially those who are first-time online banking users or who live in rural areas. As digital transactions are growing, so are cybercrime activities, driving regulations and financial institutions to take measures to further improve their fraud detection processes and cybersecurity protocols. The RBI's recent concerns over rising digital payment frauds further underscore the critical nature of this challenge (PwC India, 2025; Reuters, 2025).

1.4 Digital Banking in Rural Areas topic

Digital banking has been key in driving financial inclusion in rural India. Mobile banking applications, aadhaar based payment systems, Banking Correspondents and UPI based services enable banking facilities for the rural population without requiring to visit any banking branches. The initiatives such as BharatNet and Digital India have spurred the emergence of digital infrastructure and connectivity in certain rural regions. But low digital literacy, poor network connectivity, language barriers, and lack of awareness of cybersecurity practices remain as obstacles for effective use of Digital banking services. These factors render the rural users to be more prone to cyber fraud and financial exploitation (AISECT, 2024; Economic Sciences Journal, 2025).

1.5 Statement of the Problem

India's financial inclusion and economic development promise have been bolstered as a result of its rapid expansion of digital banking. But cyber frauds are becoming more common, creating a major concern about the trust and safety of the electronic financial environment. Especially in rural area, population is at a high risk due a lack of technological knowledge, low awareness about cyber threats and lack of access to cyber security education. Despite government efforts to promote digital financial services, there has been growing awareness of cyber fraud and this has impacted the safety and sustainability of digital financial services in rural areas. Therefore, there is a need to critically analyze the correlation between the Digital banking usage and Cyber fraud Vulnerability among rural banking customers.

1.6 Importance of the Study

This work is relevant as it can contribute to the knowledge on the opportunities and challenges for digital banking in rural India. The outcomes can assist policy makers, banks, financial regulators and cyber security agencies to establish effective strategies for enhancing digital literacy and protection measures. The study also provides an insight on what type of cyber frauds are happening for the rural users, why and how their cyber security awareness level can be improved. The study will also enhance the academic debate on digital financial inclusion and cybersecurity for the rural population in India in the broader context of cybersecurity initiatives by the Reserve Bank of India (RBI related policy initiatives, 2026; Gateway House, 2019).

1.7 The scope of the study

This paper is mainly based on the adoption of the digital banking services and cyber frauds in India with special emphasis on rural regions. It deals with different modes of banking such as internet banking, UPI, mobile banking, digital wallet, and Aadhaar-enabled banking. The study explores rural users' awareness of cyber security practices, types of cyber fraud, and factors that may lead to cybercrime victimisation. It focuses on the experiences, issues and security concerns customers of rural banks might have and does not include corporate banking or international digital payment systems.

2. Review of Literature

2.1 Concept of Digital Banking

Digital banking, or banking done virtually, is banking done without the need of a physical bank

branch. It covers internet banking, mobile banking, ATMs, EFTs, digital wallets and banking through Unified Payments Interface (UPI). Digital banking is about making things faster, easier, more accessible, and better for your customer, without increasing the costs for your financial institution. In recent years, the banking industry has undergone further changes in banking operations and customer engagement due to the integration of new technologies like Artificial Intelligence, Cloud Computing and Data Analytics (Shaikh & Karjaluo, 2015).

It has been noted that digital banking is thus a key enabler in the process of financial inclusion, which is accessing financial services by the underserved group. Mobile banking and internet connectivity have made banking possible in far-flung locations, and provided banks with the tools to make secure, real-time transactions possible. Thus, digital banking has become an integral part of contemporary financial systems, and has helped develop a cashless economy and economic growth (Ozili, 2018).

2.2 Development of Digital Banking

The digital banking transformation in India has gone through various stages. In the beginning, banking services were branch-based only, and in the late twentieth century, core banking systems, ATMs and electronic payment systems were introduced. Indian banking sector reforms and competition among banks have forced banks to adopt new technology and expanded the internet and mobile banking services (Kumar & Mohan, 2020).

A significant change has occurred, since the advent of the Digital India campaign in 2015 and the

demonetization policy in 2016 which has made digital transactions the preferred method of payment. National Payments Corporation of India (NPCI) introduced the concept of Unified Payments Interface (UPI) in the digital payments landscape, which provides a fast, secure, and interoperable platform for making payments. This has made India one of the world's largest digital payment markets and it has led to a significant increase in the adoption of digital banking in both urban and rural areas (Reserve Bank of India [RBI], 2023).

2.3 The types of cyber frauds in banking

As banking has increasingly gone digital, so has fraud against banking customers, and it has been growing at the same swift rate. Phishing is a widely used cyber fraud technique in which the attackers send fake e-mails, messages or create fake Web pages to trick people into disclosing their personal data, such as passwords, banking information or card number. Other techniques involve the use of vishing (voice phishing) and smishing (SMS phishing) using communication technologies to get confidential information from the victim (Aloul, 2012).

Cybercriminals are increasingly attacking digital payment platforms, such as OTP frauds, QR code scams, fake customer-care services, identity theft, SIM swapping, and unauthorized UPI transactions, in recent years. Social engineering refers to a type of technique that is frequently used to trick customers into providing personal information or granting fraudulent transactions. The technological advancement along with the increasing usage of online financial services has made these frauds more sophisticated which is a major challenge for

banks and regulatory authorities (Bhasin, 2016).

2.4 Inclusion of digital finance in rural India

Digital financial inclusion is an umbrella term for digital financial services that are affordable and accessible to all segments of society, especially the un-served and marginalized people. Public policies like Pradhan Mantri Jan Dhan Yojana (PMJDY), Aadhaar based payment, Direct Benefit Transfer (DBT) and mobile banking have greatly increased financial access in rural areas in India. These programs have helped millions of people who hadn't previously been served to join the formal financial system (Demirgüç-Kunt et al., 2022).

Research suggests that digital financial inclusion has helped to empower people economically, through savings, access to credit, remittances, and government welfare transfer. Increasingly, rural households are using digital payment systems for their day-to-day transactions and financial management. But the gains of digital financial inclusion require a certain level of digital literacy, digital infrastructure and trust in digital platforms. In the absence of such supporting factors, the impact of DfS in many rural areas is still limited (Ozili, 2020).

2.5 Challenges Faced by Rural Users

Even though the penetration of digital banking is improving, rural people still face various difficulties to use digital financial services. Low Internet connectivity, poor telecom systems, less education, and less digital literacy continue to be significant challenges. The rural population face challenges in comprehending the digital interface, transaction processes, and cybersecurity measures, leading to reduced trust in digital banking platforms (Sinha &

Singh, 2019).

A major issue is that there are more opportunities for cyber fraud and online financial scams than ever before. Rural customers are generally unaware of how to properly manage a secure password, how to avoid phishing attacks, how to distrust links and how to be wary of financial communications. There are still language barriers and lack of access to cybersecurity education, which further enables digital frauds. As a result, the digital divide between urban and rural people still impacts the effectiveness and security of the adoption of digital banking in India (NABARD, 2023).

2.6 Research Gap Identified

The adoption of digital banking, financial inclusion, and challenges of cybersecurity in India have been explored in depth in the existing literature. The technological acceptance, the different trends in digital payment systems and cybercrime among urban citizens and organized banking have been studied in various studies. But there have been few studies which have in detail analysed the correlation between the expansion of digital banking and the vulnerability of rural banking users to cyber fraud. However, the existing studies do not necessarily see the relationship between financial inclusion and cybersecurity, as it comes to the development of digital banking (Kumar & Mohan, 2020; Ozili, 2020).

Further, in the context of increasing adoption of digital payments, lack of empirical evidence pertaining to rural banking customers' awareness of, and behaviour towards, cyber security, and how well rural banks are cyber-secured. Cyber frauds, in particular frauds targeting the UPI customers and

the first-time digital banking customers, are constantly evolving and there's a need for more up-to-date studies especially in rural India. So, the aim of the present study is to fill this gap by studying both digital banking adoption and cyber fraud experience together and especially in the rural areas of India.

3. The purposes of the study are to:

- To examine Digital Banking services towards the rural populace of India.
- To pinpoint the major cyber frauds faced by the users of rural banking.
- To investigate the correlation between digital banking and cyber fraud.
- To determine awareness about cyber security among the rural users.
- To recommend strategies to prevent cyber scams.

4. Research Questions

- What is the Digital Banking adoption rate in rural areas?
- Which of the following cyber frauds are most common among rural users?
- What is the awareness of the rural users in cyber security practices?

5. Hypotheses

- H1: Digital banking adoption significantly influences exposure to cyber frauds.
- H2: Cybersecurity awareness significantly reduces the likelihood of cyber fraud victimization.
- H3: Demographic factors significantly affect digital banking security awareness.

6. Methodology of Research

6.1 Research outline

In the present study this descriptive and analytical research method has been adopted in order to study the emerging trend of digital banking and rising of cyber-crimes in India with special reference towards rural areas. Descriptive approach is adopted to grasp the level of adoption of digital banking, financial inclusion initiatives and cyber fraud trend, whereas Analytical approach is adopted to find out the relationship between the expansion of digital banking and cyber security issues for rural users. The research design allows picturization of the opportunities and risks in the business of providing the digital financial services in rural India (Kothari, 2004).

6.2 Nature of the Study

The study is exploratory and analytical in nature. It aims to investigate the evolution of digital banking services and analyse the emerging trends of cyber fraud crimes against the rural banking customers. The study is non-empirical and purely secondary data sources have been used. The study proposes to find out the trends, problems and policy consequences of digital banking and cyber frauds in the rural areas of India through systematic analysis of available literature, reports and statistical data (Saunders et al., 2019).

6.3 Sources of Data

As a study, it is purely secondary data that is taken from reliable and authentic sources. The reason for choosing secondary data is that it offers detailed data on growth of digital banking, financial inclusion initiatives, cybercrime statistics and rural banking development in India.

6.3.1 Secondary Data Sources

The data for the study have been collected from the

following sources:

- Annual Reports of the RBI
- NPCI reports.
- Publications of NABARD
- This is according to the Ministry of Finance and Government of India.
- Digital India Programme reports
- BharatNet project reports
- Journal articles in peer-reviewed journals.
- Banking, finance, cyber security and rural development journals indexed by Scopus.
- IMF publications
- The National Crime Records Bureau (NCRB) has started reporting on cybercrime.
- Books, conference proceedings, dissertations and working papers.
- Newspapers, magazines and online newspaper databases that are reputed.

They offer some relevant insights on the adoption of digital banking, cyber frauds, financial inclusion initiatives, and cybersecurity concerns in rural India (Reserve Bank of India, 2024; World Bank, 2022).

6.4 Period of the Study

The study mainly covers the time frame of 2020-25. The reason for selecting the period is that it witnessed all the changes in the banking landscape of India since the Digital India was introduced and the currency notes were demonetized, along with the rise of mobile banking and UPI transactions which increased significantly over the last few months. The selected timeframe has also followed a corresponding trend of cybercrime associated with financial transactions over the Digital media.

6.5 Data Collection Method

The secondary data has been obtained by the systematic review of published literature, government documents, institutional reports, statistical databases and scholarly research articles. Information relevant to the topic of Digital banking, financial inclusion, cyber frauds and rural banking issues have been explored, classified and arranged as per the objectives of the study. The collected data have been critically examined to ensure their relevance, reliability, and consistency (Creswell & Creswell, 2018).

6.6 Tools and Techniques of Analysis

Qualitative and quantitative techniques of data analysis are used. In these descriptive statistical techniques like percentage, growth rates, graphical representations, tables, and trend analysis have been used to study the digital banking growth and cyber fraud incidents in India.

The following analytical tools are used:

- Trend Analysis
- Comparative Analysis
- Percentage Analysis
- Tabular Analysis
- Graphical Representation
- Conduct a content analysis of literature.
- Interpretative Analysis

These techniques enable the identification of patterns, relationships, and emerging issues relating to the adoption of digital banking and cyber fraud risks in rural areas (Sekaran & Bougie, 2020).

6.7 Reliability and validity of data

Data has been collected only from recognized institutions and credible academic sources for

reliability and validity. The official reports of RBI, NPCI, NABARD, NCRB, the World Bank and peer-reviewed journals have been prioritized. Information from various sources has been cross verified to make sure that there are minimum errors and ensure accuracy of the analysis.

6.8 Limitations of the study

This study has some limitations. Firstly, entirely secondary data is used and there is no primary survey data from the rural bank customers. Secondly, the results are based on the accuracy and availability of published information and reports. Third, there could be an underreporting of incidents by victims, which could mean that statistics of cyber fraud are underreported. Finally, the trends identified in this study may be different after the study period as the face of digital technologies and cyber threats is constantly changing.

6.9 The conceptual framework of the study

The conceptual framework of the study is as follows

The study considers the idea that the more rural communities adopt digital banking the more financial inclusion is achieved in rural areas; and the more cyber fraud exposed. Potential factors influencing the relationship between the use of digital banking and the vulnerability to cyber fraud include cyber security awareness, cyber security regulations, digital literacy and access to the Internet. The study delves into these inter-connections and provides a comprehensive understanding of safe and secure digital banking in rural India.

7. Digital Banking Landscape in Rural India

The advent of digital banking has revolutionized the

Indian financial landscape, especially in rural regions, where traditional banking services are scarce. Since digital technology has been integrated into banking services, the rural masses can access the financial services and products through mobile phones, Internet and digital payment system. The work done by the Government, the improved telecom infrastructure, and the low cost of smart phones have been a huge boon to digital banking in rural India. Therefore, digital banking has become an important factor in helping to reduce the transaction cost and enhance the efficiency of delivering financial services and contributing to financial inclusion (Reserve Bank of India [RBI], 2023).

Digital banking has also brought in a greater share of the rural population to the formal financial system, due to the rapid growth of digital banking. Digital Payment platforms, Mobile banking apps, Aadhaar enabled services have been beneficial for rural customers to transact, avail government benefits and avail banking facilities without visiting bank premises. Yet, the non-digitization, infrastructure and awareness regarding cyber security remains to be influencing the adoption of digital banking in rural regions (NABARD, 2023).

7.1 Government Initiatives for Digital Banking

The Government of India has launched several initiatives for promoting digital banking and financial inclusion in rural India. One of the most significant of the programmes, which was started in 2015, is Digital India and is aimed to improve the digital infrastructure, increase the reach of the internet and create digital literacy in the entire country. In this context, the Government has been

encouraging digital transformation of the society and the citizens' adoption of digital technologies, including making financial transactions digital (Ministry of Electronics and Information Technology [MeitY], 2023).

Pradhan Mantri Jan Dhan Yojana (PMJDY) has also played a significant role as far as improving access of the rural population to banking services is concerned. The scheme has facilitated the opening up of millions of bank accounts for the unbanked people paving the way towards digital financial inclusion. In addition, the linkage of Aadhaar with banking services and Direct Benefit Transfer (DBT) schemes has facilitated the timely delivery of government support and benefits to beneficiaries' bank accounts, reducing leakages and promoting transparency (Government of India, 2023).

Furthermore, programmes such as the BharatNet have been undertaken to make high-speed internet connectivity available to institutions in the village as part of the campaign to close the gap between the broadband internet and the villages. The building of digital infrastructure via BharatNet has helped the uptake of mobile banking, online payments and digital financial services in remote places. These government steps collectively establish a basis for nurturing a conducive environment for digital banking in rural India, as outlined by the DoT (2023).

7.2 UPI and Mobile Banking Penetration

The Unified Payments Interface (UPI) is a digital payments platform introduced by National Payments Corporation of India (NPCI) that has transformed the Indian digital payments landscape. UPI offers an instant real-time payment platform

where the users can transfer money instantly from one bank account to another bank account via mobile devices. The simplicity, interoperability, and cost-effectiveness of its services have played a major role in its successful penetration of the market and the gradual adoption of the digital payments system by all sections of society, including the rural population (NPCI, 2024).

Mobile banking has also had significant growth in rural India with the rise in penetration of smartphones and availability of cheap internet service. Mobile apps that are User friendly have been developed by banking establishments to help their customers carry out some banking operations such as fund transfer, account management, bill payment and balance enquiry etc. Mobile banking has made banking services more accessible and less reliant on physical physical locations, thereby enhancing convenience for rural customers (RBI, 2023).

According to the recent studies, UPI transactions have grown exponentially and India has emerged as one of the biggest markets for digital payments. Rural consumers are using UPI enabled apps for various activities like buying goods, paying utility bills and receiving remittances more and more. This trend reflects a larger willingness and readiness to use digital financial services by the rural population and the ability of digital technologies to change the way banking is done in rural areas (World Bank, 2022).

7.3 Financial Inclusion and Rural Connectivity

Financial inclusion is understood to be the process of making financial services available to the everywhere and anyone at affordable prices. Digital

banking has become a powerful tool for providing financial inclusion in rural India, as it can help poor people gain access to financial services. Digital platforms allow rural individuals to use savings accounts, credit facilities, insurance products and payment services without them having to travel long distances or undergo some administrative procedures (Demirgüç-Kunt et al., 2022).

Digital financial inclusion programmes have been greatly facilitated with better rural connectivity. The cellular infrastructure, Internet connectivity, and mobile network expansion have contributed to rural peoples' integration into the formal financial system. Moreover, several innovative financial tools like banking correspondents, micro-ATMs, Aadhaar-based payment systems, and more have also helped improve financial inclusion in remote rural regions (NABARD, 2023).

Digitalization of the rural financial institutions sector has also helped in economic development of the villages by encouraging people to save money, start businesses and take loans. Small farmers, self-help groups and rural entrepreneurs are now using digital banking for financial transactions and access to other economic services. Thus, financial inclusion through digital means is not only a source of financial empowerment but also a source of overall rural development (Ozili, 2020).

7.4 The adoption of the Rural Digital Banking challenges

Even after all the improvement made, there are a number of issues that remain to the adoption of digital banking in rural India. The biggest challenges are technology and a lack of technology skills. Many rural users are not technically

knowledgeable to use the mobile app, online banking process, and cyber security threats. Lack of awareness of digital financial services may result in the lack of confidence and unwillingness to embrace the digital banking platforms (Sinha & Singh, 2019).

Issues with infrastructure are also key concerns. Although internet connectivity has much improved, to many rural areas the internet speed is slow; network coverage is weak and there is limited electricity to power the internet. These limitations impact the dependability and availability of digital banking services, especially in remote and geographically isolated areas (Department of Telecommunications, 2023).

A big hurdle is also the rise in cyber frauds against the customers of rural banks. Fraudsters use phishing emails, fake customer service calls, OTP scams, and fake UPI transactions which are common frauds owing to lack of cybersecurity awareness among users. These events can cause economic damage, lose trust in digital banking and diminish uptake. Therefore, it is essential to have a robust consumer protection mechanism and enhance the awareness programme on cybersecurity measures to sustain the development of rural Digital Banking (Reserve Bank of India, 2024).

Digital banking adoption also is impacted by language barriers and socio-cultural factors. Digital banking applications and financial education materials are largely in English and in a handful of regional languages; which is limiting access to diverse rural populations. Furthermore, some groups at the population level continue to be influenced by the reluctance to use new technology,

and favor cash payment. Responding to these is the need for cooperation and collaboration between different stakeholders such as the government, financial institutions and technology providers for an inclusive and secure digital banking ecosystem.

8. Cyber Fraud in rural areas is analyzed

Digital banking has contributed immensely to access to finance services and financial inclusion in the rural areas of Indian subcontinent. But the growing adoption of digital channels has also put the clientele of rural banks at risk of cyber fraud of all kinds. Rural users are especially susceptible to cybercrime operations due to their limited digital literacy, lack of cybersecurity awareness, and reliance on mobile-based financial transactions. The technological vulnerabilities and the lack of awareness among people can lead to unauthorized access to their personal and financial information, leading to significant monetary losses and eroding the trust in digital banking systems (Reserve Bank of India [RBI], 2024).

Policymakers, financial institutions, and law enforcement have all found cyber fraud to be a significant issue. The frauds are of growing sophistication and in a fast-changing world with quick adoption of digital payment methods like UPI and mobile banking, frequency and complexity of frauds have risen. By grasping the nature and scope of these cyber-crimes, including their impact on the rural population, effective preventive measures can be implemented, and digital financial security can be enhanced (National Crime Records Bureau [NCRB], 2023).

8.1 Major Types of Cyber Frauds

- **Phishing-** One of the most popular cyber-crime methods used to trick people into providing their username, password, debit card and banking information is called 'phishing'. The fraudulent emails, messages or website links normally come from reputable financial institutions. Unsuspecting users are convinced to input personal information, and it's then made use of for unapproved financial transactions. Such deceptive practices are frequently used on the target population, which is the rural users with little knowledge about online security measures (Aloul, 2012).
- **Vishing-** Voice phishing, also known as vishing, is a type of fraud that occurs when criminals give pretentious calls impersonating bank representatives, government employees or customer service representatives. The caller tries to befriend the victim and asks for confidential details like the account number, ATM pin, OTPs or Aadhaar details etc. Rural customers are especially susceptible to these calls, as they might assume they are a legitimate call and accept without checking who is calling. With mobile phones being used widely in the rural area, the problem of vishing is a big threat (Bhasin, 2016).
- **Smishing-** Smishing is a phishing attack carried out via a Short Message Service (SMS) message. Fraudsters send misleading text messages with links, false offers, false account verification requests or false warnings of account suspension. Clicking

these links or filling out the requested information can potentially compromise users' financial information. The rising adoption of smartphones and mobile banking apps has helped the rise of smishing attacks in rural areas (Jain & Gupta, 2020).

- **UPI Fraud-** By providing a smooth and practical platform for transactions, UPI has completely changed the digital payments scene in India. But cyber-criminals are now tricking the UPI-using users with fake payment requests, fake notifications of payments, and unauthorised access to UPI accounts. Many victims think they are getting paid when they approve payment requests. These misconceptions have contributed to the rapid rise of UPI fraud in India, making it a significant issue in digital financial crime (NPCI, 2024).
- **QR Code Scam-** QR code scams involve the distribution of fake QR codes, purportedly to help people pay, claim refunds or rewards. The victims are asked to use a digital payment application to scan the code. The transaction does not result in the victim receiving funds, rather the money is moved from the victim's account to the fraudster's account. QR code-based transactions are especially vulnerable to such frauds, with rural users being particularly susceptible due to less familiarity with how these transactions work (RBI, 2024).
- **OTP Fraud-** One-Time Password (OTP) fraud is a common type of cybercrime where

fraudsters trick the victim into disclosing the OTPs sent to their registered mobile numbers. Cybercriminals typically impersonate bank staff, customer service or government personnel and tell customers that OTP verification is required to activate a service or increase security on their accounts. The OTP is revealed and then any type of unauthorized transaction can be made. This fraud is taking advantage of the lack of awareness regarding banking security measures (NCRB, 2023).

- **Fake Loan Applications-** With the emergence of fake mobile applications and fraudulent websites, cybercriminals have started to provide instant loans that require little paperwork. The victims are coerced to provide their personal information, bank account details and identity documents. Most often, fraudsters take your personal details or ask for up-front processing fees, but don't actually grant you a loan. Such deceptive schemes are especially prevalent with rural people who need fast cash (Cyber Peace Foundation, 2023).
- **Social Engineering Attacks-** Social engineering attacks are psychological exploitation of people with the intention to make them reveal information or take actions that facilitate the attack. Scammers use emotions like fear, urgency, trust and greed to trick. This is most commonly in the form of fake lottery schemes, emergency assistance requests and impersonation of relatives or government officials. Social

engineering is still very effective because it attacks human behavior instead of the vulnerability of a technology (Mitnick & Simon, 2011).

8.2 The causes for cyber frauds in rural areas

The growing prevalence of cyber frauds in rural India can be attributed to various factors. Low digital literacy is one of the most important factors. A large number of rural users have little understanding of how digital banking works, cybersecurity and how to prevent online fraud. Consequently, they can be unwittingly disclosing confidential data or may be receiving fraudulent messages (Sinha & Singh, 2019).

An additional driver is a lack of cyber security awareness. Secure passwords, phishing detection, privacy settings and transaction verification procedures are unknown to many of the rural banking customers. This ignorance presents chances for cybercriminals to trick users into being victims of their own devices. In addition, there is lack of cybersecurity education and awareness programmes, which aggravates the situation (NABARD, 2023).

Technological and infrastructural challenges also play a role in increasing cyber fraud risks. Users can be vulnerable to cyber threats due to shared devices, insecure internet connections, outdated software, and compromised security measures. Moreover, due to language barriers and reliance on informal sources of information, rural customers are not able to comprehend the security tips provided by banks and regulatory bodies (RBI, 2024).

8.3 The impact on the rural banking customers

The financial, psychological and social impact of

cyber fraud on rural banking customers is very serious. The immediate consequences are financial losses from unauthorized transactions, fraudulent withdrawals, or the theft of personal information. A small amount of money lost for an economically vulnerable family can have a significant impact on livelihoods and household stability (NCRB, 2023).

Beyond economic damage, victims are likely to suffer emotional distress, anxiety and loss of trust in digital financial services. Multiple cyber fraud cases can lead to fear and distrust of digital banking platforms, deterring customers from using e-payment systems. Such a lack of confidence will affect financial inclusion efforts and hamper the adoption of digital banking in rural areas (Ozili, 2020).

Cyber fraud impacts also on the general economic development goals. The planned efforts by the government to encourage cashless transactions and digital financial inclusion can be hampered if rural customers do not adopt digital transactions for security reasons. Hence, it is paramount to tackle cyber fraud to maintain public confidence and the continued success of digital banking programmes (World Bank, 2022).

8.4 Examines Case Studies of Selected Cyber Fraud Incidents

• Case 1: UPI Payment Request Fraud

A farmer in a rural district got a call from someone who said that he was interested in buying agricultural produce. On this, the fraudster sent a request for a UPI payment and asked the farmer to approve it for the payment. The farmer didn't know the distinction between a payment request and a payment receipt, and authorized the payment

request, which resulted in money being deducted from his account. The case highlights the dissatisfaction of rural consumers with the digital payment systems due to lack of knowledge, which results in monetary loss (NPCI, 2024).

- **Case 2: OTP-based banking fraud**

A rural customer was called by a person who pretended to be a representative from a bank, stating that the customer's bank account would be blocked if he or she did not complete a verification process quickly. The fraudster asked the customer to provide an OTP that he received on his registered mobile phone number. Just a few days later, someone was doing transactions on the victim's account without his permission. This incident underscores the power of social engineering attacks and the importance of enhancing customer awareness of OTP confidentiality, per RBI 2024.

- **Case 3: The scam involves a fake loan application**

An unemployed rural youth downloaded a mobile application that provides personal loans with attractive interest rate. Aadhaar information, bank account information and advance processing fee was sought in the application. The Applicant did not get the loan nor did he get back the fee. The fraudsters used the personal information later for additional fraudulent activities. This case illustrates the growing threat posed by fake financial applications and fraudulent lending platforms (Cyber Peace Foundation, 2023).

Analysis of these incidents shows that the lack of digital literacy among the rural population, cyber security awareness and exploitation of trust by cybercriminals are the major motivations behind

cyber frauds in rural India. To minimize cyber fraud risks and ensure a safe adoption of digital banking services in rural areas, it is therefore crucial to strengthen digital education, organize cybersecurity awareness campaigns and improve consumer protection measures.

9. Analyse and interpret data

The RBI, NPCI, NCRB, NABARD, World Bank, and peer-reviewed research journals are some of the sources of secondary data used in this study. Data collected have been analyzed to get a clear picture of the digital banking services, financial inclusion and Cyber Frauds in India especially in rural areas. To reach meaningful conclusions about the opportunities and challenges related to the adoption of digital banking, trend analysis, comparative analysis, and interpretative techniques have been used (Reserve Bank of India [RBI], 2024).

9.1 The Growth of Digital banking services

Secondary data analysis shows that digital banking services have significantly grown in India in the last ten years. With the implementation of the Digital India initiative, the adoption of smartphones, low-cost Internet connectivity, and the launch of UPI, digital transactions have increased significantly in the country. The RBI reports have shown that the digital payment volumes have consistently grown at double-digit rates per year, reflecting a significant transition towards cashless financial transactions.

The advent of mobile banking and internet banking services has also helped more rural population to engage with formal financial services. The expansion of digital financial services in rural areas has also been facilitated by government-led initiatives like PMJDY, Aadhaar-based payment

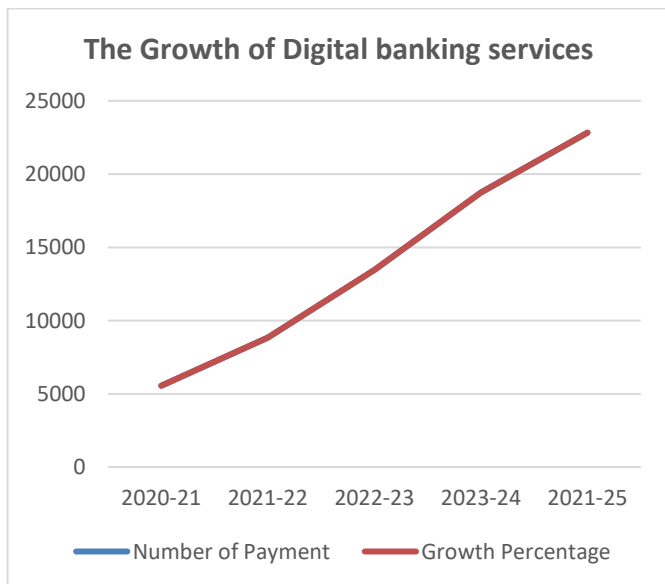
systems, and Direct Benefit Transfer (DBT) schemes (Government of India, 2023).

Table: 01

The Growth of Digital banking services

S.No.	Years	Number payment details	Growth Rate %
1.	2020-21	5554	21%
2.	2021-22	8839	59%
3.	2022-23	13462	62%
4.	2023-24	18737	39%
5.	2024-25	22831	22%

Source: Ministry of Finance Year Ender 2025: Department of Financial Services, Updated on: 10th Jan 2026, by PIB Delhi.



Interpretation

These data point to significant growth in digital banking transactions in India during the period of 2020–21 to 2024–25. The number of payment transactions grew from 5,554 in 2020–21 to 22,831 in 2024–25, highlighting a boost in the use of digital banking services. However, the growth rate was highest in 2022-23 at 62% and was at 59% in 2021-22, driven by the greater use of UPI, mobile banking and digital payment platforms. While the growth rate gradually slowed down to 22% in 2024-25, the overall upward trajectory highlights the sustained growth of digital banking and the increasing acceptance of cashless transactions in India.

9.2 Digital Banking Services Uses: UPI

As per reports available, UPI has proven to be the most popular digital payment company in India. The features of simplicity, speed and convenience of UPI have helped it to gain traction among urban, as well as rural users. Mobile banking apps, digital wallets, online banking platforms, and Aadhaar-based payment solutions are also gaining traction for everyday banking activities like fund transfers, utility bill payments, and payments to merchants (NPCI, 2024).

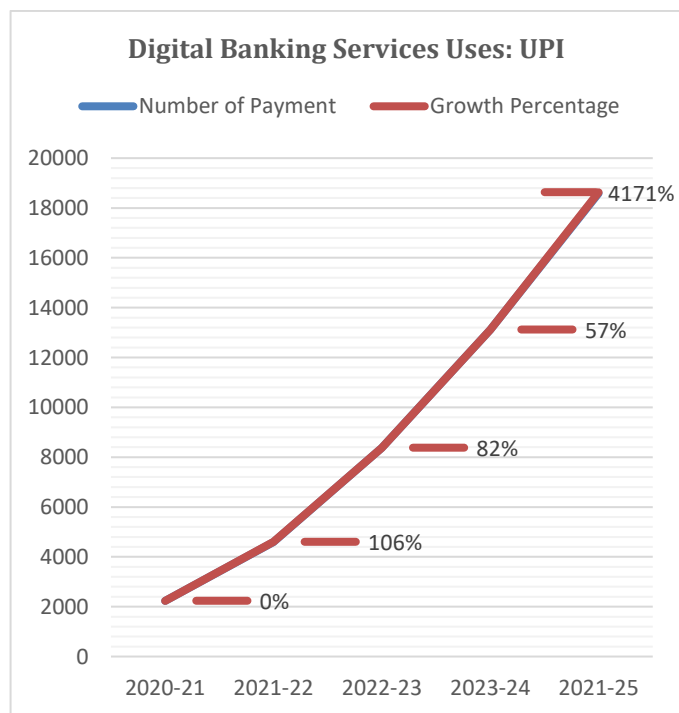
The rural customers have mainly used digital banking services for receiving benefit from the government, agricultural payments, receiving remittances and daily activities. The level of usage, however, is determined by digital literacy, internet access, education level, and their ownership of a smartphone. The evidence indicates that adoption of digital banking has risen significantly, however, there are still some differences between rural and urban areas in terms of the frequency of and sophistication for using digital financial services (NABARD, 2023).

Table: 02

Digital Banking Services Uses: UPI

S.No.	Years	Number payment details	Growth Rate %
1.	2020-21	2233	-
2.	2021-22	4597	105.87%
3.	2022-23	8375	82.19%
4.	2023-24	13116	56.61%
5.	2024-25	18587	41.71%

Source: Ministry of Finance Year Ender 2025: Department of Financial Services, Updated on: 10th Jan 2026, by PIB Delhi.



Interpretation

The table shows the impressive growth of digital transactions through UPI in 2020-21 and 2024-25 as compared to the preceding years. The adoption of digital payment systems in India has risen significantly, with the number of payment transactions going up from 2,233 in 2020–21 to 18,587 in 2024–25. The UPI's usage increased at the fastest rate of 105.87% in 2021–22 as the penetration of the internet and smartphones, along with government measures to encourage digital payments, drove the rapid growth of the segment. The growth rate has been gradually decreasing till 2024-25 at 41.71%, but the increase in the number of transactions also shows the popularity and usage of UPI as a preferred payment platform. This is an indicator of the growth of the digital banking ecosystem in India and the gradual move towards a cashless society.

9.3 Awareness Level of Cyber Security

Based on the literature surveyed in this study, it was found that the awareness of cyber security still has relatively low level among rural banking users compared to urban banking users. Some studies have claimed that there is a lack of awareness among consumers on how to keep their passwords secure, phishing, OTP confidentiality, fraudulent links and safe procedures for digital transactions,

especially among rural consumers. This lack of awareness makes them vulnerable to cyber fraud and financial exploitation (Sinha & Singh, 2019).

Despite the ongoing awareness campaigns carried out by banks, regulatory authorities and government agencies, there are major knowledge gaps. There have been reports that a large proportion of customers are not familiar with the official banking security measures and use unofficial channels of information when operating digital financial services. Therefore, improving cyber security education is an essential need to make the use of digital banking safe in rural areas (RBI, 2024).

Awareness Level of Cyber Security

Table No. 3

S.No.	Awareness Initiative	Purpose
1	Cyber Dost Campaign	Public awareness regarding cyber safety and fraud prevention
2	National Cyber Crime Reporting Portal	Online reporting of cybercrime complaints
3	Helpline Number 1930	Immediate reporting of financial cyber frauds
4	Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)	Quick freezing of fraudulent transactions
5	Cyber Awareness Programs	Digital literacy and cybersecurity education for citizens
6	Social Media Awareness Campaigns	Dissemination of fraud prevention information

Source: Results of Comprehensive Modular Survey: Telecom, 2025 (January – March, 2025)

Interpretation

The Government of India has taken a multi-dimensional approach to enhance the awareness of citizens about cyber

security. Awareness sprees, Cyber Dost initiative, National Cyber Crime Reporting Portal and helpline 1930 have been launched to sensitize the public about Cyber menace and to enable timely reporting of fraud incidents. The steps are to minimize losses and raise awareness on digital security, especially first-time digital banking users and rural population.

9.4 To Analyze Cyber Fraud Incidents

Secondary data shows that the number of cyber frauds related to digital banking and online financial transactions has been steadily growing. Along with the increase in the number of transactions, the number of attacks using techniques like phishing, OTP frauds, QR code attacks, fake loan applications, UPI-related frauds and social engineering have also increased. The reports put out by NCRB reveal a significant rise in the number of cybercrime cases that involved financial fraud in recent years (NCRB, 2023).

Rural users, especially, seem to be at a high risk because of low digital literacy and low-level cybersecurity awareness. Often, fraudsters take advantage of trust, urgency, and misinformation to trick victims into giving out private data or approving illegitimate activity. As cybercriminal techniques continue to evolve, there is a growing need for robust consumer protection measures and improved digital security frameworks (Cyber Peace Foundation, 2023).

Analyze Cyber Fraud Incidents

Table No- 4

S.No.	Indicator	Reported Data
1.	High-value cyber fraud cases in FY 2024	29082 Cases
2.	High-value cyber fraud cases in FY 2023	6699 Cases
3.	Increase in cyber	More than 4 times

	fraud cases	
4.	Estimated losses due to cyber frauds	Approximately US \$20 million
5.	Major fraud categories	UPI fraud, phishing, impersonation scams, OTP Fraud, Social Engineering attacks
6.	Reporting mechanism	Helpline 1930 and Cybercrime Portal

Source: Results of Comprehensive Modular Survey: Telecom, 2025 (January – March, 2025)

Interpretation

It shows that cyber fraud incidents have risen significantly, in line with the growth of digital banking and digital payments. The number of high-value cyber fraud cases rose over fourfold from 6,699 in FY 2023 to 29,082 in FY 2024. This is blamed on rising digital transactions, rise in internet penetration, and lack of cyber awareness among users. Phishing, impersonation, OTP theft and social engineering are some of the most popular approaches fraudsters use when targeting banking customers. The results indicate the need for effective cyber literacy initiatives and improved cybersecurity measures, particularly for financial institutions and farmers in rural regions, where the adoption of digital banking is growing.

10. Analytical Findings

The secondary data gathered from RBI, NPCI, NCRB, NABARD, reports of ministry of finance and other reliable sources provide some key observations on the adoption of digital banking and cyber frauds in India, especially in the rural areas.

10.1 Major Findings

(1) Key Advances in Digital Banking

Services- The study revealed that digital banking services are growing at a fast pace in India over the years 2020-21 to 2024-25. Digital payment transactions increased from 5,554 crore in 2020–21 to 22,831 crores in 2024–25. The year-on-year growth rate peaked at 62% in 2022–23, reflecting a

quicken pace of digital financial service uptake in the wake of greater smartphone penetration, internet access, and government programs encouraging digital transactions.

- (2) **The dominance of UPI as a digital payment platform-** UPI turned out to be the most popular digital payment method available in India. In 2020-21, there were 2,233 crore transactions on UPI, which rose to 18,587 crore transactions in 2024-25. Rapid acceptance of UPI was seen in 2021-22 with the highest growth rate at 105.87% by both urban and rural users. While annual growth rates in later years were less, the rise in transaction volume has been steady, suggesting that consumers are not losing trust in UPI-based payments.
- (3) **Improvement in Financial Inclusion-** In rural India, the government has taken significant efforts toward enhancing financial inclusion, including through the launch of various initiatives like the Pradhan Mantri Jan Dhan Yojana, Aadhaar-based payment systems, Direct Benefit Transfer, and Digital India. Digital banking has made banking services available to rural households, allowing them to access banking services, receive benefits from the government, make financial transactions, and transfer money without relying on brick-and-mortar banks.
- (4) **The 'Digital Divide in Rural Areas' continues to exist-** Though much has been achieved, there are still inequities between rural and urban people. Low digital skills,

lack of internet connectivity, lower penetration of smart phones and education levels remain factors that continue to affect the frequency and sophistication of the adoption of digital banking among the rural population.

- (5) **Inadequate Cybersecurity Awareness-** The study reveals that rural banking users are not very aware of Cyber security. Many of customers do not know about safe password practices, phishing attacks, OTP confidentiality, fraudulent links, QR code frauds, and security measures in digital banking. This ignorance can lead to falling prey to cyber frauds and monetary losses.
- (6) **Initiatives for Government Cybersecurity Awareness-** Among other initiatives, the Indian government has started the Cyber Dost Campaign, the National Cyber Crime Reporting Portal, the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), Helpline Number 1930, and social media awareness campaigns. These initiatives are proactive in preventing cybercrime and safeguarding consumers.
- (7) **Rapid increase in cyber fraud incidents-** The study showed a significant increase in the number of cyber fraud cases related to digital financial transactions. From 6,699 cases in FY 2023, high-value cyber fraud cases jumped to 29,082 cases in FY 2024, marking a more than four-fold rise in a year. This trend highlights the growing threat

posed by cybercriminals in the expanding digital economy.

- (8) **Growing financial losses due to cyber fraud-** Estimated losses have been heavy to the tune of some US \$20 million to the cyber frauds. There are more opportunities for cyber criminals to exploit vulnerabilities in digital payment systems and user behavior as a result of the growth in digital transactions.
- (9) **UPI Related and Social Engineering Fraud are predominant-** The most frequently reported type of cyber frauds are UPI frauds, Phishing attacks, Impersonation scams, OTP frauds, QR code scams and social engineering attacks. These scams mostly occur through exploiting vulnerabilities in people, not in technology, as they require cyber security awareness and digital literacy.
- (10) **The need for enhanced consumer protection mechanisms-** The results show that digital banking adoption is growing at a very fast pace and that the protection of consumers is not yet fully effective and needs to be strengthened to respond to the new cyber risks. Safe digital banking practices require effective awareness campaigns and cybersecurity education as well as quick fraud response mechanisms.

10.2 Discussion of Findings

The study findings show that in the last 10 years India has made tremendous progress with respect to digital banking and the achievement of financial inclusion. Indeed, these substantial digital transactions growth and the use of UPI can be seen

as a success of the various government initiatives such as Digital India, PMJDY, DBT, and Aadhaar-based payment systems. These have transformed the banking environment, which includes facilitating the banking services to be accessible, low cost and convenient particularly to rural population.

The study also shows that UPI has now emerged as a backbone of the India's digital payment system. The number of UPI transactions has grown exponentially, showing the public's acceptance and trust in digital payment platforms. Today, the rural people use UPI services and mobile banking for receiving subsidy, agricultural payments, remittance and day to day transactions, increasing the overall financial inclusion and economic participation.

But the study points to a key issue surrounding the swift expansion of digital banking. As digital financial services have grown, so have the number of cyber fraud incidents. The sharp surge in high-cost cyber frauds from FY 2023 to FY 2024 clearly signals the cybercriminals' growing efforts to take advantage of the expanding digital landscape. This indicates that if there is no proper and sufficient awareness of cybersecurity, an opportunity of digital financial inclusion can also bring vulnerable people to risks.

The results also show that fraudulent activities in the cyber world have disproportionately affected the rural banking customers as they are less digitally literate and less aware about cyber security measures. Many farmers don't know to take simple security measures like protecting OTPs, checking links, and verifying QR codes, and they often don't know what phishing is. Therefore, fraudsters are able to carry out successful attacks using trust and

misinformation.

While the Government of India has taken multiple measures in the field of cybersecurity awareness, the fact that cyber fraud is still prevalent means there is a need for a further push in awareness initiatives that can be expanded and localized. Cybersecurity education should be included in financial education campaigns and be communicated in regional languages for better outreach among rural population.

In conclusion, the study finds that digital banking has played a significant role in promoting financial inclusion and economic development in India. However, a balanced strategy is needed for sustainable growth of digital banking, encompassing technological innovation, cybersecurity awareness, regulatory oversight, and consumer protection. In order to ensure the sustainability and security of the digital banking ecosystem in India, it becomes imperative to strengthen the digital literacy and cybersecurity preparedness of the rural users.

11. Conclusion

This study was particularly focused on the development of digital banking and the increase in Cyber Frauds in India, especially in the rural regions. Nevertheless, the analysis conducted on secondary data obtained from RBI, NPCI, NCRB, NABARD and from the reports of the Ministry of Finance, the publications of the World Bank and other relevant literature reveals that digital banking has brought revolution in financial sector, and has played significant role in the financial inclusion process.

The results indicate that digital banking transactions

have seen an outstanding increase between 2020–21 and 2024–25. The journey towards cashless economy has been expedited with the advent of unified payments interface (UPI), mobile banking, internet banking and digital wallets. Government initiatives like Digital India, Pradhan Mantri Jan Dhan Yojana (PMJDY), Aadhaar enabled payment systems, BharatNet and Direct Benefit Transfer (DBT) have been pivotal in bringing digital financial services to the rural and underserved communities.

The study also demonstrates that UPI has emerged as the most popular digital payment system due to its easy and convenient usage, speed and accessibility. The surge in UPI transactions is indicative of the trust that users have in digital payment systems and the effectiveness of India's digital payment infrastructure.

Unfortunately, as digital banking has grown and evolved, so have the cyber frauds. Analysis of phishing attacks, OTP frauds, UPI frauds, QR code scams, impersonation frauds and social engineering attacks has been found to be high. A special vulnerability is that of the rural users, given their low level of digital literacy, the lack of awareness of cybersecurity, limited access to digital education, and dependence on informal sources of information. The research results show that digital banking has contributed to financial inclusion and economic involvement, but has some cyber security challenges that endanger the sustainability of digital financial services. Therefore, the future of digital banking in India's rural areas will rely on technological progress and the development of effective cybersecurity protocols, consumer

protection policies, and regulatory frameworks. Hence, there is a need to strike a balance between financial inclusion and digital security, ensuring trust and the safe and sustainable future of digital banking in India.

12. Recommendations

According to the study's results, the following recommendations are suggested to improve the security and effectiveness of digital banking services in rural areas:

- (1) Regular digital literacy programmes should be undertaken in rural areas by the government agencies, banks, educational institutes, and non-governmental organizations. These programs should emphasize usage of digital banking, online payment systems, and secure digital transactions. Elderly people, women, farmers and first-time digital banking users should be given special attention.
- (2) Village level workshops, community meetings, social media campaigns, radio and other local language communication channels should also be expanded to spread cybersecurity awareness initiatives. Awareness campaigns need to inform users about phishing attacks, the confidentiality of OTPs, QR scams, fake loan applications and other new cyber threats.
- (3) To further improve the infrastructure in villages, the government should continue its efforts by funding schemes like BharatNet or other plans to expand broadband connectivity. Equitable access to digital banking services is contingent on reliable

internet connectivity, uninterrupted electricity supply and affordable digital devices.

- (4) Banks are required to regularly enhance their cybersecurity and fraud detection. To safeguard customers against cyber threats, multi-factor authentication, biometric verification, real-time transaction alerts, AI-driven fraud monitoring, and secure mobile banking apps should be widely adopted.
- (5) Digital banking applications, awareness materials and cybersecurity advisories should be provided in regional and local languages. Language will enable rural customers to have a better understanding of banking procedures, security guidelines, etc., and hence reduce the risk of fraud.
- (6) Village or block level special cyber assistance and digital support centers can be set up to enlighten on digital banking services, cyber security practices and cyber-crime reporting procedures. These centres can help you report your cases of fraud as soon as possible and provide you with the support you need.
- (7) Reporting cyber fraud through Helpline Number 1930 and National Cyber Crime Reporting Portal should be improved further in terms of accessibility and ease. Registration of complaints, investigation and resolution will be fast, improving public confidence in digital financial systems.
- (8) To tackle cyber fraud challenges, the cooperation and collaboration between banks, fintech, regulators, law enforcement,

educational institutions and community organizations are key. A coordinated effort will help build comprehensive strategies for prevention, detection and response.

- (9) Cybersecurity awareness and consumer protection should be included as an integral part of future financial inclusion policies. Increased access to digital financial services (DFS) without a corresponding boost in security risks could put users, especially in rural settings, in a more vulnerable position.
- (10) As cyber risks are constantly evolving, ongoing research is needed to track trends in fraud, levels of cyber security awareness and the impact of policy interventions. Periodic research will enable policymakers and financial institutions to have evidence-based plans to protect digital banking users.
- (11) The potential of digital banking in rural India is vast, and it has the potential to significantly drive financial inclusion and economic development in the region. But all of those benefits can only be realized if a range of measures are implemented at the same time to improve cybersecurity awareness, cybersecurity literacy, technological infrastructure and consumer protection. These steps will help in the establishment of a safe, inclusive and sustainable digital banking system for everyone.

References

AISECT. (2024). *Digital banking in rural India 2024*. <https://aisect.org/digital-banking-in-rural-india-2024/>

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176–183.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176–183.

Bhasin, M. L. (2016). Cybercrime and cyber fraud in India: Problems and prevention. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(3), 224–230.

Bhasin, M. L. (2016). Cybercrime and cyber fraud in India: Problems and prevention. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(3), 224–230.

Bhattacharjee, A. (2012). *Social science research: Principles, methods, and practices* (2nd ed.). University of South Florida.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Cyber Peace Foundation. (2023). *Digital fraud trends and cybersecurity awareness in India*. Cyber Peace Foundation Research Report.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank.

Gateway House. (2019). *A cybersecurity agenda for India's digital payment systems*. Gateway House Research Paper.

Jain, A., & Gupta, M. (2020). Mobile banking security challenges and fraud prevention mechanisms. *International Journal of Information Systems and Technology*, 5(2), 85–97.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International Publishers.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International Publishers.

Kumar, R., & Mohan, D. (2020). Digital banking and financial inclusion in India: Opportunities and challenges. *International Journal of Banking, Risk and Insurance*, 8(2), 45–58.

Kumar, U. (2025). *Bridging the gap: Digital payments and financial inclusion in rural India*. International Journal of Economic Development Research.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Wiley Publishing.

National Bank for Agriculture and Rural Development (NABARD). (2023). *Status of digital financial inclusion in rural India*. NABARD Research Report.

National Bank for Agriculture and Rural Development. (2023). *Status of digital financial inclusion in rural India*. NABARD.

National Bank for Agriculture and Rural Development. (2023). *Status of digital financial inclusion in rural*

- India. NABARD.
- National Crime Records Bureau. (2023). *Crime in India 2023: Cybercrime statistics*. Ministry of Home Affairs, Government of India.
- National Crime Records Bureau. (2023). *Crime in India 2023: Cybercrime statistics*. Ministry of Home Affairs, Government of India.
- National Payments Corporation of India. (2024). *Annual report 2023–24*. NPCI.
- National Payments Corporation of India. (2024). *UPI safety awareness and transaction security guidelines*. NPCI.
- Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, 18(4), 329–340.
- Ozili, P. K. (2020). Financial inclusion research around the world: A review. *Forum for Social Economics*, 50(4), 457–479.
- Ozili, P. K. (2020). Financial inclusion research around the world: A review. *Forum for Social Economics*, 50(4), 457–479.
- PwC India. (2025). *Combating payments fraud in India's digital payments landscape*. PricewaterhouseCoopers India.
- Reserve Bank Information Technology Pvt. Ltd. (ReBIT). (2018). *The evolving digital financial landscape in India: Technology interventions for strengthening the digital payment systems*. ReBIT Research Publication.
- Reserve Bank of India. (2023). *Report on trends and progress of banking in India 2022–23*. Reserve Bank of India.
- Reserve Bank of India. (2023). *Report on trends and progress of banking in India 2022–23*. Reserve Bank of India.
- Reserve Bank of India. (2024). *Annual report 2023–24*. RBI.
- Reserve Bank of India. (2024). *Annual report 2023–24*. Reserve Bank of India.
- Reuters. (2024, August 26). *India to launch platform for rural, small business lending, central bank governor says*.
- Reuters. (2025, February 7). *India central bank governor cautions lenders against rising digital frauds*.
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.
- Sekaran, U., & Bougie, R. (2020). *Research methods for business: A skill-building approach* (8th ed.). Wiley.
- Shaikh, A. A., & Karjaluo, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, 32(1), 129–142.
- Sharma, R., & Singh, P. (2025). *Challenges in implementing digital banking services in rural India*. *Economic Sciences Journal*, 5(2), 45–59.
- Sinha, P., & Singh, S. (2019). Digital literacy and rural banking adoption in India. *International Journal of Rural Management*, 15(2), 168–184.
- World Bank. (2022). *Digital financial services and financial inclusion in developing economies*. World Bank.
- Ministry of Finance Year Ender 2025: Department of Financial Services, Updated on: 10th Jan 2026, by PIB Delhi, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2213154®=48&lang=2>
- Results of Comprehensive Modular Survey: Telecom, 2025 (January – March, 2025), Published on: 29 MAY 2025 4:00PM by PIB Delhi. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2132330®=48&lang=2>
