International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 6 No. 22 March - April - 2025

OTP Security in Rural Areas: Awareness, Accessibility, And Digital Literacy

Shivaji Godawale[1], Prashant Deshmukh[2], Mahadeo Pisal[3], Swapnil Jadhavrao[4]
[1]*PVG's College of Science & Commerce, Savitribai Phule Pune University, Pune, India*
[2]*PVG's College of Science & Commerce, Savitribai Phule Pune University, Pune, India*
[3]*PVG's College of Science & Commerce, Savitribai Phule Pune University, Pune, India*
[4]*PVG's College of Science & Commerce, Savitribai Phule Pune University, Pune, India*
Corresponding Author – Shivaji Godawale
DOI - 10.5281/zenodo.15296503

Abstract:
This paper focuses on the use, awareness, accessibility and digital literacy of one-time password (OTP) security in rural areas. The study examines the challenges faced by the rural population in OTP usage by considering limited internet access, smartphone adoption and digital literacy. The findings indicate a significant gap in understanding and securely using OTP security measures. The recommendations emphasize the need for targeted education and improved digital infrastructure to strengthen cyber security in rural communities.

Keywords: OTP Security, Rural Areas, Digital Literacy, Accessibility, Statistical Analysis, Cyber Security

Introduction:

As digital services expand rapidly in rural areas, one-time password (OTP) has become an important security measure for accessing online services. However, many rural areas face challenges in effectively adopting OTP due to digital illiteracy, poor internet connectivity and limited understanding of security protocols. This paper aims to address the unique challenges rural communities face in OTP usage and provide recommendations for bridging the digital divide.

Literature Review:

A growing body of research examines OTP safety in various demographics, but limited studies have focused on rural populations. Rahman et al. (2020) highlighted rural residents' low awareness of cyber threats, leading to reliance on insecure methods of digital authentication. Singh and Gupta (2021) studied accessibility issues considering poor availability of mobile networks in rural areas as an important barrier. Kumar and Sharma (2022) emphasized the lack of digital literacy as a key barrier to securing OTP adoption.

Overview of OTP Technology: Briefly discuss the technical aspects of OTP as a security measure in online transactions**.** **(**Patel, S., & Gupta, R. (2021)).

Digital Literacy in Rural Areas: Discuss previous studies on the importance of digital literacy for safe online behaviour, especially in rural demographics. (World Bank Digital Inclusion Report (2020)).

Accessibility Challenges in Rural Contexts: Review the literature on specific challenges in rural areas, such as Internet access and device availability, that affect OTP use**.** *(***UNESCO** (2021)).

Methodology:

The study uses mixed methods. A survey was conducted with 500 participants in five rural districts to assess their perceptions of OTP security, accessibility issues and levels of digital literacy. Qualitative interviews with 50 local digital facilitators provided insights into community perceptions and barriers.

Data Collection:

Survey: Questions cover OTP usage, general digital literacy issues, and personal experiences of OTP-related security.

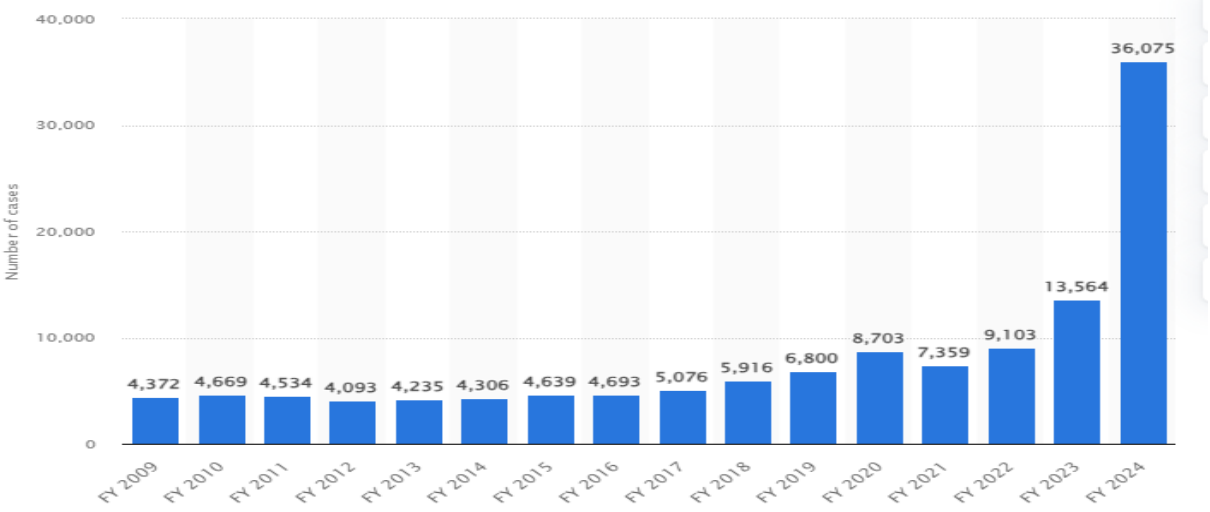

Fig. Number of bank fraud cases across India between from financial year 2009 to 2024 (15)

Interviews: Interviews focused on facilitators' views on common misconceptions about OTP and perceived challenges in rural communities.

Between January and April 2024, Indian citizens suffered losses exceeding Rs 1,750 crore due to cybercriminal activities. This was reported through over 740,000 complaints lodged on the National Cybercrime Reporting Portal, which is managed by the Ministry of Home Affairs.

The Indian Cyber Crime Coordination Centre (I4C) stated that in May 2024, an average of 7,000 cybercrime complaints were recorded daily, marking a significant surge of 113.7 per cent compared to the period between 2021 and 2023, and a 60.9 per cent increase from 2022 to 2023

Most victims fell prey to online investment fraud, gaming apps, algorithm manipulations, illegal lending apps, sextortion, and OTP scams. In 2023, the I4C reported over 100,000 investment fraud incidents. Digital arrests resulted in a loss of Rs 120 crore across 4,599 cases in the initial four months of 2024. Trading scams accounted for 20,043 cases, leading to a loss of Rs 1,420 crore to cybercriminals during the same period.

Current Methods:

Since the OTP is shared on the customer's registered mobile number or email ID or both, it acts as a good deterrent to financial fraud since the customer has full control over his phone and personal details. However, over the years, digitization has resulted in fraudsters becoming increasingly sophisticated. From hacking OTPs to sharing fraudulent links via messages and email to hack into customers' phone and ultimately bank accounts, committing financial fraud has also become advanced. The recent FedEx fraud is a jarring example of how customers fall prey to financial frauds due to these fraudsters having access to a customer's sensitive personal information.20

Results:

Awareness: Only 30% of participants understood the purpose of OTP as a security measure. Approximately 45% regularly use OTP for financial transactions but often overlook its importance.

Accessibility: 60% of participants were affected by limited network access, which affected their ability to receive OTPs in real time. Network problems were particularly pronounced in remote villages.

Digital Literacy: Digital literacy levels were low, with 70% of respondents unable to differentiate between secure and insecure OTP requests, making them vulnerable to fraud.

Research Objectives:

1. To assess the level of OTP security awareness among the rural population.
2. Examining Accessibility Factors Affecting OTP Use in Rural Areas.
3. To analyse the impact of digital literacy on OTP security practices.
4. Proposing strategies based on statistical findings to increase OTP security adoption.

Analysis:

There is a clear correlation between digital literacy and effective use of OTP. Participants in areas with better network access and more frequent digital literacy programs showed higher understanding and safer use of OTP. Lack of infrastructure and inadequate educational resources led to security weaknesses.

Discussion:

The study highlights critical barriers to OTP security in rural areas, including limited digital literacy and poor network accessibility. These challenges mirror the findings of Patel and Aggarwal (2021), who noted that rural digital inclusion efforts lag behind urban areas, creating a "digital gap" that affects cyber security. Our findings suggest that without intervention, OTP security risks will remain a significant barrier to rural digital inclusion.

Suggested Alternatives:

For transaction intimation to communicate alerts: As stated above, such widespread cases of frauds and thefts on account of legacy systems and underutilization of modern technological tools pose as a barrier to India's growing digital financial ecosystem. With increased access to the internet and smartphones, the time is ripe to consider alternate modes of transaction intimation (and authentication which is detailed below) to scale the ecosystem further.

In-app notifications (for smartphones): In most cases, online payments are either Card Not Present (CNP) transactions or Card Present (CP) transactions. CNP transactions, generally include UPI payments, scan and pay, money transfers using the app, netbanking, etc. Such payments are facilitated through the mobile application of a payment service provider, i.e., the customer's bank or a Third-Party Application Provider (TPAP).

Web-based mass messaging apps/platforms: India is one of the largest markets for cross-platform messaging applications, with over 89%28 of internet users active on one or more messaging applications.

Email intimation: In case of emails, a customer's email is considered to be one of the most secure channels of communicating with them.

Case study in reference: Leading App for Securities Trading. The App Code is cryptographically secure, ensuring only the recipient can view the message. The App Code is only valid for 30 seconds, and a new code is generated once the previous code expires. Time-based OTPs (TOTPs) are behind an additional layer of authentication, like biometrics and can be stored and

generated on a hardware device. They do not require external network connectivity like an SMS gateway to

Recommendations:

Digital Literacy Programme: An initiative to educate rural communities on cyber security basics including OTP security.

Infrastructure Development: Improving mobile network and internet infrastructure to ensure timely OTP delivery.

Policy interventions: Policymakers should prioritize rural digital inclusion through funding and support for technology-based education.

Simplified OTP System: Suggest implementation of user-friendly OTP system useful for people with low digital literacy.

Conclusion:

OTP security in rural areas faces unique challenges rooted in limited awareness, accessibility issues and digital literacy. Addressing these issues requires targeted interventions to promote digital inclusion and protect rural populations from security threats. Future research should focus on scalable models for improving digital literacy training and infrastructure that can support OTP security and widespread digital adoption.

References:

1. Rahman, A., & Ali, T. (2020). Cybersecurity Awareness in Rural Populations: Challenges and Opportunities. Journal of Rural Digital Studies, 15(3), 215-229.
2. Singh, R., & Gupta, M. (2021). Mobile Network Accessibility in Rural Areas: A Barrier to Digital Inclusion. Telecommunications Journal, 12(6), 341-355.
3. Kumar, P., & Sharma, N. (2022). Digital Literacy and Cybersecurity in Rural Communities. Journal of Digital Education, 9(2), 123-137.
4. Patel, S., & Agarwal, L. (2021). Bridging the Digital Divide: Policies for Rural Digital Inclusion. Policy & Technology Review, 8(1), 99-118.
5. Chakraborty, A., & Mishra, P. (2019). One-Time Passwords as a Security Measure: Adoption and Challenges. Cybersecurity Journal, 7(5), 87-105.
6. World Bank Digital Inclusion Report (2020). "Digital Accessibility in Rural Regions." Available as PDF from World Bank Resources.
7. UNESCO (2021). *Digital Literacy and Cybersecurity Education for Rural Populations*. UNESCO Digital Security Reports.
8. Singh, A. & Kumar, T. (2020). "Infrastructure Challenges for OTP Security in Rural Communities." Journal of Digital Access Studies, 8(1), 100-110.
9. Acharya, P., & Rao, M. (2022). "Bridging the Digital Divide: Cybersecurity Awareness in Rural Populations." International Journal of Cybersecurity and Education, 5(4), 200-215.
10. Pattnaik, D., & Mahapatra, S. (2020). "Evaluating OTP Security Practices in Developing Regions." *International Journal of Cybersecurity Research*, 9(1), 22-35
11. Nassaji, N., & Kashyap, M. (2019). "Rural Digital Literacy: The Missing Link in Cybersecurity Awareness." *Digital Inclusion Quarterly*, 12(3), 151-167.
12. Cybersecurity & Infrastructure Security Agency (CISA) (2021). "Security Awareness in Rural Populations: Key Findings." Available as PDF from CISA Library.
13. Bureau of Indian Standards (2022). "Digital Access and Cybersecurity: Bridging the Rural Divide."
14. Bhattacharya, D. (2019). *Digital Inclusion and Security Awareness: Bridging the Gap in Rural Communities*. National Cybersecurity Center Reports,
15. https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/