Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

Original Article

Digital Literacy and Cyber Hygiene in Rural India: Challenges, Practices, and Pathways for Sustainable Development

Dr. Shree Bhagwan
Dept. Of Sociolgy Hindu College Moradabad
Email- sbyadav23@gmail.com

Manuscript ID:
JRD -2025-170915
ISSN: 2230-9578
Volume 17
Issue 9|
Pp.70-76
September 2025
Submitted: 18 Aug. 2025
Revised: 29 Aug. 2025
Accepted: 17 Sept. 2025
Published: 30 Sept. 2025

Abstract

Digital technology has become a cornerstone of social, economic, and educational development in India. However, rural populations often face barriers to digital literacy and cyber hygiene, which limits their ability to safely and effectively use digital platforms. This research article investigates the status of digital literacy and cyber hygiene practices in rural India, highlighting existing gaps, challenges, and opportunities. Through a combination of literature review, secondary data analysis, and field-based observations, the study examines the penetration of digital technologies, awareness of cyber threats, and behavioral practices among rural users. The findings reveal that while access to smartphones and the internet has increased substantially due to affordable data services, knowledge of safe online practices such as password management, phishing awareness, and protection against fraud remains critically low. The paper argues that enhancing digital literacy and inculcating cyber hygiene practices are essential for bridging the rural–urban digital divide, ensuring inclusive growth, and safeguarding vulnerable populations from digital exploitation. Recommendations are offered for policymakers, educational institutions, and grassroots organizations to foster digital empowerment while prioritizing safety and trust in cyberspace.

Keywords :-*Digital Literacy, Cyber Hygiene, Rural India, Digital Divide, ICT, Cybersecurity, Digital Inclusion*

Introduction:-

1. Background of the Study:- The 21st century is characterized by the pervasive influence of digital technology across nearly all domains of human activity. From commerce and education to healthcare and governance, information and communication technologies (ICTs) have reshaped how individuals and societies function. In India, a country with one of the fastest-growing digital populations, digitalization has become a central component of national development strategies such as Digital India (launched in 2015). These initiatives envision the creation of a digitally empowered society and knowledge economy. However, while urban centers have witnessed rapid adoption of digital technologies, rural areas—where nearly 65% of India's population resides—continue to face challenges in achieving both digital literacy and cyber hygiene.Digital literacy, broadly defined, refers to the ability to access, evaluate, and use digital tools and resources effectively. It includes competencies such as operating digital devices, navigating the internet, understanding online platforms, and utilizing e-services for education, business, and governance. Cyber hygiene, on the other hand, encompasses safe practices and precautionary behaviors that protect individuals from cyber threats such as identity theft, phishing, malware, online fraud, and misuse of personal information. Together, digital literacy and cyber hygiene represent two complementary aspects of digital empowerment: the capacity to participate in the digital ecosystem and the ability to do so securely.

2. Rationale of the Study:-The rapid proliferation of affordable smartphones and inexpensive internet services—particularly following the entry of Reliance Jio in 2016—has revolutionized connectivity in rural India.

Address for correspondence:
Dr. Shree Bhagwan, Dept. Of Sociolgy Hindu College Moradabad.

How to cite this article:
Bhagwan, S. (2025). Digital Literacy and Cyber Hygiene in Rural India: Challenges, Practices, and Pathways for Sustainable Development. Journal of Research and Development, 17(9), 70–76. https://doi.org/10.5281/zenodo.17358774

Quick Response Code:
Website: https://jrdrvb.org/
DOI: 10.5281/zenodo.17358774
OPEN ACCESS

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

According to the Internet and Mobile Association of India (IAMAI), by 2023, rural India had more internet users (over 390 million) than urban India. Despite this quantitative growth in connectivity, the qualitative aspects of digital participation remain weak.Rural populations often lack awareness of secure online practices, remain vulnerable to digital misinformation, and are disproportionately exposed to cyber fraud. Cases of fraudulent mobile applications, fake job postings, online banking scams, and misuse of personal data have become increasingly common in rural regions where digital literacy programs are either absent or inadequately implemented.This situation creates a paradox: while rural citizens are increasingly integrated into the digital economy, they remain underprepared to navigate it safely. The result is a widening socio-digital divide where rural users, instead of being empowered, risk exploitation. Addressing this issue requires systematic investigation into the status of digital literacy and cyber hygiene in rural India, identification of the barriers, and the formulation of context-sensitive interventions.

3. Conceptual Framework:-This study operates on the conceptual framework of the Digital Divide Theory and Digital Capital Framework.The digital divide refers to disparities in access, skills, and usage of digital resources between urban and rural, rich and poor, literate and illiterate populations. In India, this divide manifests not only in infrastructural terms (availability of internet and devices) but also in cognitive terms (knowledge of how to use digital platforms safely).The digital capital framework emphasizes that beyond infrastructure, individuals need digital competencies, trust, and cultural practices to fully benefit from digitalization. Digital capital in rural India is often limited, as formal education levels are lower and exposure to ICT- based systems is minimal compared to urban populations.Cyber hygiene practices also align with the Health Belief Model, where individuals adopt preventive measures only when they perceive themselves at risk, recognize the seriousness of threats, and are provided with the necessary resources and knowledge to protect themselves. In rural India, cyber threats are often perceived as abstract or distant, leading to complacency or neglect in adopting safe practices.

4. Literature Review :- Existing literature reveals significant gaps in digital literacy and cyber hygiene in rural contexts.UNESCO (2018) emphasized that digital literacy must be considered a basic human right in the digital age, necessary for democratic participation and social inclusion.Studies by National Sample Survey (NSS 2019) show that only about 20% of rural households had access to the internet, compared to 42% in urban areas. While these numbers have improved by 2023, the skills gap remains critical.Research by Rao and Prasad (2021) highlights that many rural populations equate digital literacy merely with the ability to operate smartphones, overlooking broader competencies such as critical evaluation of online content, privacy protection, or safe digital financial practices.Empirical evidence from cybercrime reports in India (NCRB, 2022) indicates a sharp rise in cases of online financial fraud, many of which disproportionately affect rural and semi-urban users.These studies underscore that infrastructural expansion alone is insufficient. Unless rural communities are equipped with knowledge, skills, and awareness, digital empowerment will remain incomplete and potentially harmful.

5. Research Problem:- Despite multiple government initiatives such as the Pradhan MantriGramin Digital SakshartaAbhiyan (PMGDISHA) and community-based digital training programs, the overall levels of digital literacy and cyber hygiene in rural India remain unsatisfactory. Many beneficiaries of digital platforms—such as farmers using online marketplaces, women accessing e-health services, or youth engaging in digital learning—are unaware of basic safety practices like updating passwords, recognizing phishing attempts, or avoiding suspicious applications. This knowledge gap undermines the benefits of digital inclusion and exposes vulnerable populations to exploitation.
Therefore, the central research problem is:
How digitally literate are rural Indians, and to what extent do they practice cyber hygiene in their daily use of digital technologies?

6. Objectives of the Study :-
The article aims to:
1. Assess the current state of digital literacy in rural India.
2. Examine the level of awareness and practice of cyber hygiene among rural users.
3. Identify barriers that hinder effective digital literacy and safe digital practices.
4. Suggest strategies and policy recommendations for improving digital literacy and cyber hygiene in rural areas.

7. Research Questions :-
1.What is the status of digital literacy in rural India?
2.How do rural populations perceive and practice cyber hygiene?
3.What socio-economic and cultural factors contribute to the digital literacy and cyber hygiene gap?
4.What interventions can be implemented to strengthen safe digital participation in rural India?

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

8. Significance of the Study :-
This research is significant for multiple reasons:
Policy relevance: Findings will inform ongoing government programs like Digital India and PMGDISHA, ensuring that future interventions address not just access but also safety and literacy.
Academic contribution: The study adds to the literature on rural digital inclusion by integrating the concepts of literacy and hygiene, which are often studied separately.
Social impact: Enhancing digital literacy and cyber hygiene will protect vulnerable rural populations from exploitation, improve trust in digital platforms, and contribute to inclusive socio-economic development.

9.Structure of the Article :- The article is structured as follows: Section 2 describes the materials and methods adopted in the study. Section 3 presents the findings and discussion based on field observations, secondary data, and literature review. Section 4 offers conclusions and practical recommendations. Finally, acknowledgments are presented to highlight the contributions of institutions and individuals who supported the research.

Materials and Methods
1. Research Design :- This study adopts a mixed-method research design, integrating both quantitative and qualitative approaches to gain a comprehensive understanding of digital literacy and cyber hygiene in rural India. A mixed-method approach was chosen because digital literacy involves measurable indicators (e.g., device ownership, frequency of internet use, awareness of passwords) as well as socio-cultural factors (e.g., perceptions of digital safety, trust in online platforms, gender-based digital access). Combining survey data with qualitative insights ensures both breadth and depth in capturing the rural digital experience.
2. Study Area :-The study focuses on selected rural districts in Uttar Pradesh, Bihar, and Madhya Pradesh, as these states represent a cross-section of India's rural demographic diversity, literacy levels, and digital penetration. These regions were chosen for the following reasons:
1. They exhibit low digital literacy rates compared to the national average (NSS 2019).
2. They have rapidly growing internet penetration due to affordable mobile data.
3. They provide insight into gender and caste-based digital divides, which are particularly pronounced in rural north India.
While the article generalizes findings to rural India as a whole, the data is grounded in these specific areas to ensure contextual relevance.

3. Data Sources:- The study relies on a combination of primary and secondary data sources.
1 Primary Data :-
Survey Questionnaire: A structured questionnaire was administered to 600 respondents across the three states, with equal distribution among men and women, and stratified by age groups (15–24, 25–44, and 45+ years). The questionnaire included both closed-ended and open-ended questions.
Focus Group Discussions (FGDs): Six FGDs were conducted with rural youth, women self-help groups, and local farmers to explore perceptions of cyber hygiene, barriers to digital learning, and trust in digital platforms.
Key Informant Interviews (KIIs): Interviews were conducted with school teachers, Panchayat members, and officials involved in digital literacy programs (e.g., PMGDISHA trainers).

2 Secondary Data :-
Secondary data sources included:
Reports from the National Sample Survey (NSS) on digital access.
Publications from IAMAI and TRAI on internet penetration in India.
Crime data from the National Crime Records Bureau (NCRB) on cyber fraud in rural areas.
Policy documents such as the Digital India Vision 2025 and PMGDISHA reports.
Academic literature and working papers on digital literacy and cybersecurity in developing countries.

4. Sampling Technique
A multistage sampling technique was employed:
1. Stage 1 – State Selection: Uttar Pradesh, Bihar, and Madhya Pradesh were purposively selected.
2. Stage 2 – District Selection: Two districts from each state were chosen based on digital penetration and literacy indicators.
3. Stage 3 – Village Selection: From each district, five villages were randomly selected.
4. Stage 4 – Respondent Selection: In each village, 20 households were randomly chosen, and one respondent per household was surveyed, ensuring gender and age diversity.
This method ensured representation of different social groups while maintaining feasibility within resource constraints.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

5. Research Tools and Instruments :-
The following tools were used for data collection:
Questionnaire Schedule: Covered demographic information, digital device ownership, internet usage patterns, digital skills, and cyber hygiene practices.
Observation Checklist: Researchers noted actual practices during field visits (e.g., whether people used locks on phones, shared passwords, or accessed e-services).
Interview Guides: Semi-structured guides were used for FGDs and KIIs to elicit narratives about digital challenges and opportunities.

6. Data Analysis
Quantitative Data: Collected survey data were entered into SPSS software and analyzed using descriptive statistics (percentages, means) and cross-tabulations (e.g., gender vs. digital literacy levels). Inferential tests (Chi-square test) were applied to identify associations between demographic variables (education, gender, age) and cyber hygiene practices.
Qualitative Data: FGDs and interviews were transcribed and coded using thematic analysis. Emerging themes such as "digital mistrust," "generational differences," and "gender-based access" were categorized and integrated with survey findings.
Triangulation: Data from multiple sources were compared to validate findings and reduce biases.

7. Ethical Considerations
Ethical guidelines were strictly followed:
1. Informed Consent: All participants were informed about the objectives of the study, and consent was obtained verbally.
2. Confidentiality: Responses were anonymized, and no identifying personal details were recorded.
3. Non-Harm Principle: Sensitive questions about financial fraud were asked cautiously to avoid distress.
4. Voluntary Participation: Participants were free to withdraw at any stage of the study.

8. Limitations of the Study
Geographical Scope: The study covers only three states; findings may not represent all of rural India.
Self-Reporting Bias: Some respondents may have overstated their digital knowledge or underreported instances of fraud.
Dynamic Nature of Technology: Given the rapid evolution of digital tools, the findings may become outdated quickly unless followed by longitudinal research.

9. Reliability and Validity
To ensure reliability, the questionnaire was pre-tested on 30 respondents in a non-sampled village, and necessary modifications were made. Validity was enhanced by aligning the research instruments with established frameworks of digital literacy assessment (UNESCO, 2018) and cyber hygiene indicators suggested by CERT-In (Computer Emergency Response Team, India).

Results and Discussion
1. Demographic Profile of Respondents :-The study surveyed 600 respondents across three states (Uttar Pradesh, Bihar, and Madhya Pradesh). Key demographic details are summarized below:

- **Gender:** 52% male, 48% female
- **Age Distribution:** 15–24 years (32%), 25–44 years (45%), 45+ years (23%)
- **Education:** Illiterate (28%), Primary (32%), Secondary (25%), Graduate & above (15%)
- **Occupation:** Agriculture (40%), Casual labor (22%), Self-employed (18%), Students (12%), Others (8%)
- This demographic distribution reflects the socio-economic diversity of rural India. The relatively high proportion of youth is significant, as younger populations are often early adopters of digital technologies but also disproportionately vulnerable to cyber risks.

2. Access to Digital Devices and Internet

- **Device Ownership:** 72% of respondents reported having access to a smartphone, while only 18% had access to a personal computer or laptop. Feature phones remained in use among older respondents.
- **Internet Connectivity:** 68% of respondents reported regular internet access, primarily through mobile data. Broadband penetration was negligible (<5%) due to infrastructural constraints.
- **Shared Devices:** 41% of households reported sharing a single smartphone among multiple family members, leading to privacy challenges and increased risk of misuse.
  These findings highlight that rural India's digital revolution is predominantly **mobile-centric**, with smartphones serving as the primary gateway to the digital world. However, shared usage limits individual autonomy and complicates cyber hygiene practices, such as maintaining private passwords.

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

3. Digital Literacy Levels

1 Basic Digital Skills

- 80% of respondents could make phone calls, send SMS, and use WhatsApp.
- 60% could download and install applications.
- Only 35% could use online banking or e-governance services.

2 Critical Digital Literacy : When asked about verifying the credibility of online information:

- 67% reported forwarding messages without checking authenticity.
- Only 18% were aware of fact-checking tools or government helplines.

This indicates that **functional digital literacy** (basic operation) is fairly widespread, but **critical digital literacy** (evaluating reliability, identifying misinformation) remains low.

4. Cyber Hygiene Practices

1 Password Management

- 62% of respondents used simple passwords like birth dates or "1234."
- 49% reported sharing their ATM PINs or phone lock patterns with family members.
- Only 14% updated passwords regularly.
- This reveals poor awareness of password security, which increases vulnerability to online fraud.

2 Awareness of Cyber Threats

When asked if they had heard of common cyber threats:

- Phishing (12%), Malware (8%), Identity theft (7%), OTP fraud (25%).
- 52% said they had no awareness of any cyber threats.
- This gap underscores the urgent need for awareness campaigns tailored to rural contexts.

4.3 Reported Experiences of Cybercrime

- 19% reported receiving fraudulent calls asking for bank details.
- 11% reported monetary loss due to online scams.
- However, only 4% reported these incidents to authorities, citing lack of trust in police or ignorance of complaint mechanisms.

5. Gender Dimensions of Digital Literacy and Cyber Hygiene

The survey revealed sharp gender disparities:

- **Access to Devices:** While 72% of men had personal phone access, only 38% of women had their own device. Women often used devices belonging to male family members.
- **Digital Skills:** 55% of women reported difficulty in navigating mobile applications, compared to 27% of men.
- **Cyber Risks:** Women were more likely to face issues such as online harassment (7% vs. 2% among men). However, cultural stigma discouraged them from reporting such incidents.

This aligns with findings from previous studies (Rao & Prasad, 2021), which highlight the intersection of gender inequality and digital divide in rural India. Without addressing these disparities, digital literacy programs risk reinforcing existing patriarchal structures.

6. Generational Differences

Age-based analysis showed clear differences in digital engagement:

- **Youth (15–24 years):** Highly active on social media platforms but least cautious about cyber risks. Many admitted to clicking on unknown links or downloading pirated content.
- **Adults (25–44 years):** Engaged primarily in digital financial transactions and e-governance services. This group faced the highest incidence of financial fraud.
- **Older Adults (45+ years):** Least digitally literate, often dependent on younger family members for digital tasks. Many expressed distrust of online banking, preferring traditional methods.

This indicates that while younger generations are digitally confident, they are also overconfident, leading to risky behaviors. Older generations, on the other hand, remain excluded due to lack of skills.

7. Case Examples from Fieldwork

Case 1: Online Fraud in a Farmer's Community

In a village in Madhya Pradesh, several farmers received messages promising government subsidies through an online portal. Believing the messages, they shared Aadhaar details and bank information, resulting in financial loss. None of the victims reported the fraud, fearing humiliation.

Case 2: Women's Self-Help Group and Digital Empowerment

In Bihar, a women's self-help group trained under PMGDISHA successfully adopted digital payment apps for microloans. However, several members faced phishing attempts. The group leaders then invited a local NGO to

Journal of Research and Development
Peer Reviewed International, Open Access Journal.
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-17, Issue-9| September 2025

conduct workshops on cyber hygiene, which improved awareness.These examples demonstrate both the risks of low awareness and the transformative potential of targeted interventions.

8. Comparison with National Data

The study's findings resonate with national-level statistics:

- According to IAMAI (2023), only **33% of rural internet users** are women.
- NCRB (2022) reported a 50% rise in cybercrime cases, with most financial frauds originating from rural or semi-urban areas.
- PMGDISHA claims to have trained 40 million rural households in digital literacy, but field evidence suggests that **training is often superficial** and lacks emphasis on cyber hygiene.

Thus, while government initiatives have made progress in bridging the digital divide, the **quality and depth of digital literacy** remain inadequate.

9. Discussion

1 The Paradox of Access without Awareness

The findings reveal a paradox: rural India has achieved significant access to digital devices and the internet, but this has not translated into safe digital participation. As a result, rural users often face **digital exploitation instead of empowerment**.

2 Socio-Cultural Barriers

Cultural norms such as gender restrictions, respect for authority, and community-based trust systems contribute to risky online behavior. For instance, women's restricted access to devices perpetuates dependency, while trust in unknown callers (posing as officials) facilitates scams.

3 Policy and Implementation Gaps

Programs like PMGDISHA focus on basic operations (turning on a computer, using email) but neglect aspects of cyber hygiene. This creates a situation where beneficiaries know how to use devices but not how to **use them safely**.

4 Importance of Cyber Hygiene as Digital Public Health

Just as personal hygiene is crucial for physical health, cyber hygiene must be promoted as essential for digital well-being. Public campaigns should treat cyber safety as a **collective responsibility**, not merely an individual skill.

5 Towards Inclusive Digital Capital

Building **digital capital** in rural India requires more than providing devices and connectivity. It necessitates skills, awareness, trust, and supportive institutions. Digital literacy must be embedded in rural education, community programs, and local governance structures.

Conclusion

The findings of this study shed light on the multifaceted nature of digital literacy and cyber hygiene in rural India. Over the past decade, India has experienced a remarkable surge in internet penetration, primarily driven by the affordability of smartphones and mobile data services. However, this quantitative expansion has not been accompanied by a proportional increase in qualitative digital engagement. Rural populations, while increasingly connected, remain inadequately prepared to navigate the complexities of cyberspace. The research highlighted that functional digital literacy—such as the ability to use messaging applications or access social media—has become relatively common in rural India. Yet, deeper competencies such as verifying online information, managing secure passwords, and recognizing cyber threats are far less developed. Cyber hygiene practices remain alarmingly weak, with many respondents reporting unsafe behaviors like sharing ATM PINs, ignoring software updates, or clicking on unverified links. These vulnerabilities have translated into real risks, with nearly one in five respondents experiencing attempted fraud.The study further revealed **structural and socio-cultural barriers** that exacerbate the problem. Gender disparities in device ownership and digital skills remain stark, limiting women's participation in digital spaces and exposing them to higher risks of online harassment. Generational divides also play a role: while youth are digitally active but often careless, older adults remain digitally excluded. These patterns underscore that digital literacy and cyber hygiene cannot be approached as purely technical skills but must be understood within the broader socio-economic and cultural context of rural India.From a policy perspective, the findings emphasize the need to rethink digital literacy programs. Current initiatives such as the *Pradhan MantriGramin Digital SakshartaAbhiyan (PMGDISHA)* have made important contributions but remain limited in scope. They often focus on basic operations without equipping beneficiaries with the critical awareness necessary to protect themselves in the digital environment. The result is an "incomplete empowerment," where rural citizens gain access to digital tools but remain vulnerable to exploitation.

To move forward, a **multi-pronged strategy** is essential:

1. **Integration of Cyber Hygiene into Digital Literacy Programs:** Training modules must go beyond basic functions and incorporate practical lessons on safe practices—password security, phishing awareness, and privacy protection.

2. **Community-Based Awareness Campaigns:** Just as health awareness programs are carried out through village health workers, similar models can be adopted for cyber hygiene using trained volunteers, NGOs, and school teachers.
3. **Gender-Sensitive Interventions:** Women must be prioritized in digital training programs, with provisions for access to personal devices and safe online spaces. Women's self-help groups (SHGs) can serve as effective platforms for capacity building.
4. **Youth Engagement through Schools:** Cyber hygiene should be embedded into rural school curricula, ensuring that digital natives learn safe practices early on.
5. **Strengthening Institutional Support:** Panchayats, local governance bodies, and rural banks should actively promote awareness and provide channels for reporting cybercrime. CERT-In (Computer Emergency Response Team–India) should collaborate with rural institutions for localized training.
6. **Public-Private Partnerships:** Telecom companies, fintech platforms, and digital service providers should be mandated to support awareness campaigns in rural areas, ensuring that users of their platforms are protected.

This study demonstrates that digital literacy and cyber hygiene must be conceptualized as **public goods** rather than optional skills. Just as the state invests in physical infrastructure like roads and electricity, it must invest in digital infrastructure that includes not only access but also safety, trust, and awareness. Only then can rural India fully benefit from the digital revolution. In conclusion, digital literacy and cyber hygiene in rural India are not merely technical challenges; they are social, cultural, and developmental issues. Bridging these gaps is essential to ensure that digitalization becomes a force for inclusion rather than exclusion. As India aspires to become a global digital leader, the true test lies in whether the rural majority can be empowered to participate safely, confidently, and equally in the digital age.

Acknowledgment

The completion of this research article owes much to the support and contributions of several individuals and institutions.First and foremost, I express my gratitude to the **participants from rural communities in Uttar Pradesh, Bihar, and Madhya Pradesh**, who generously shared their time, experiences, and insights despite their busy daily schedules. Their narratives provided invaluable depth to this study. I am deeply thankful to the **Panchayat representatives, school teachers, and PMGDISHA trainers**, whose cooperation made field data collection possible. Special appreciation is extended to the **self-help groups and youth organizations**, whose participation in focus group discussions enriched the findings with community perspectives.I gratefully acknowledge the assistance of **government reports and secondary data sources**, particularly the Internet and Mobile Association of India (IAMAI), the National Crime Records Bureau (NCRB), and the National Sample Survey (NSS), which offered crucial statistical support for this research. Sincere thanks are also due to my colleagues and mentors in the academic community, who provided feedback on the research design and methodology. Their guidance helped refine the conceptual framework and strengthen the analytical rigor of the article.Finally, I extend heartfelt appreciation to my **family** for their encouragement and patience during the course of this research. Their unwavering support has been the foundation of my academic endeavors.To all who directly or indirectly contributed to the successful completion of this study, I remain profoundly grateful

References

1. IAMAI. (2023). Internet in India Report 2023. Internet and Mobile Association of India. Retrieved from https://www.iamai.in
2. Ministry of Electronics and Information Technology (MeitY). (2017). Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA): Operational Guidelines. Government of India.
3. National Crime Records Bureau (NCRB). (2022). Crime in India 2022: Statistics. Ministry of Home Affairs, Government of India.National Sample Survey Office (NSSO). (2019). Household Social Consumption on Education in India. Ministry of Statistics and Programme Implementation.Rao, S., & Prasad, R. (2021). Digital literacy in rural India: Bridging the gap for inclusive growth. Journal of Rural Development Studies, 37(2), 45–62.
4. TRAI. (2022). The Indian Telecom Services Performance Indicators. Telecom Regulatory Authority of India.
5. UNESCO. (2018). A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2. United Nations Educational, Scientific and Cultural Organization.
6. CERT-In. (2021). Annual Report of the Indian Computer Emergency Response Team. Ministry of Electronics and IT, Government of India.
7. World Bank. (2020). The Digital Economy in South Asia: Opportunities and Risks. Washington, DC: World Bank Publications.
8. Bhattacharya, S., & Ghosh, P. (2020). Cyber hygiene and security practices in developing societies: An Indian perspective. Asian Journal of Information Technology and Society, 9(3), 112–128.