

Digital Literacy as a Tool for Combating Online Fraud in Rural Communities

M. Dhavapriya

Assistant Professor, UG Computer Science (SF), NGM College, Pollachi.

Abstract- The expansion of digital payments, mobile banking, online public services, and smartphone-based communication has created new opportunities for rural communities in India. At the same time, the increasing use of digital platforms exposes users to online fraud, including phishing, impersonation, fraudulent payment requests, deceptive links, and unauthorised financial transactions. Digital literacy can help individuals recognise suspicious activities, protect personal information, verify digital communications, and respond appropriately when fraud occurs. However, the ability to operate a smartphone does not necessarily indicate the ability to use digital services safely. This research proposal aims to examine the role of digital literacy in combating online fraud among adults in rural Tamil Nadu. The study will combine a review of existing literature with a proposed questionnaire survey investigating digital literacy, cybersecurity awareness, fraud-recognition skills, preventive practices, and knowledge of reporting procedures. A conceptual framework is proposed to examine how digital literacy may relate to fraud-prevention capability, with digital access, educational background, prior exposure to fraud-awareness programmes, and confidence in digital services considered as relevant contextual factors. A multistage sampling approach and descriptive and inferential statistical methods are proposed, subject to feasibility and institutional approval. The study is expected to contribute evidence for designing accessible, community-based, Tamil-language digital literacy programmes. Since primary data have not yet been collected, no empirical findings are claimed.

Keywords - Digital literacy, online fraud, cybersecurity awareness, rural communities, digital financial inclusion, fraud prevention, rural Tamil Nadu.

I. INTRODUCTION

Digital technologies have become increasingly important in everyday activities, including communication, education, banking, shopping, access to government services, and financial transactions. In rural communities, digital platforms can reduce geographical barriers and provide access to services that previously required travel or direct interaction with institutions. Mobile devices and digital payment systems can also support financial inclusion by enabling users to conduct transactions more conveniently.

However, the benefits of digital participation are accompanied by cybersecurity risks. Users may receive fraudulent messages, encounter impersonation attempts, click deceptive links, disclose confidential information, or approve transactions without adequately verifying the recipient. Fraudsters may exploit urgency, fear, trust in familiar institutions, or limited understanding of digital security practices.

Digital literacy provides a useful foundation for addressing this challenge. In the present study, digital literacy refers to the ability to access and operate digital technologies, evaluate online information, recognise potential threats, protect personal information, and make informed decisions when using digital services. Cybersecurity literacy represents a more specific dimension involving knowledge and practical skills related to digital safety.

Importantly, digital literacy should not be reduced to the ability to use a smartphone or complete an online transaction. A user may be comfortable with mobile applications yet have difficulty identifying a fraudulent message or understanding the consequences of sharing a one-time password. Effective digital participation therefore requires technical skills, critical judgement, awareness of common fraud patterns, and knowledge of appropriate reporting procedures.

Afzal et al. (2025) examined the relationship between cybersecurity awareness, cyber fraud, trust, and digital financial inclusion in rural India. Their findings indicate that cyber fraud can undermine trust and the intention to adopt payment banking, whereas cybersecurity awareness and trust are positively associated with adoption. This research provides a relevant foundation for investigating the role of digital literacy in rural communities.

Similarly, Gogoi et al. (2025) evaluated a digital literacy training programme among adolescent girls in rural Jharkhand. Their quasi-experimental study reported improvements in digital literacy scores in the intervention group. Although that study did not specifically evaluate online fraud prevention among adult residents of Tamil Nadu, it demonstrates the feasibility of assessing community-based digital literacy interventions in a rural Indian context.



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 09, September 2026)

Against this background, the proposed study focuses on rural Tamil Nadu and examines how digital literacy may help residents recognise online fraud, adopt safer practices, and respond appropriately to suspected incidents. The study will also consider practical barriers such as language, educational background, access to training, and confidence in digital services.

II. STATEMENT OF THE PROBLEM

The increasing use of digital financial services has made it important for users to understand the risks associated with online transactions. Rural residents may encounter digital fraud through text messages, telephone calls, messaging applications, payment requests, fraudulent websites, or individuals impersonating bank employees and government officials.

The ability to access digital technology does not automatically provide the knowledge needed to identify these threats. Some users may be unfamiliar with warning signs such as requests for confidential authentication details, suspicious links, unexpected payment demands, or instructions to act immediately. Others may recognise that a transaction is suspicious but may not know how to contact their bank or submit a complaint through an appropriate official channel.

Digital literacy initiatives often emphasise device operation, internet access, and the use of online services. However, practical fraud-recognition skills, safe transaction behaviour, and reporting knowledge also require attention. Training may be less effective if it is not adapted to local language, educational background, accessibility needs, and everyday digital activities.

Existing research has addressed cybersecurity awareness and digital financial inclusion in rural India, while digital literacy intervention research has demonstrated the potential value of structured training in rural settings (Afzal et al., 2025; Gogoi et al., 2025). Further context-specific investigation is needed to understand the relationship between different dimensions of digital literacy and fraud-prevention capability among adult residents of rural Tamil Nadu.

The central problem addressed by this proposal is: To what extent are digital literacy and cybersecurity awareness associated with online fraud recognition, preventive practices, and reporting knowledge among adults in rural Tamil Nadu? The proposed study will investigate this question through a literature review and a questionnaire-based survey. It will not assume that low digital literacy is the sole cause of fraud or that literacy alone can eliminate fraudulent activity.

III. REVIEW OF RELATED LITERATURE

A. Digital Literacy and the Digital Divide

Digital literacy involves more than physical access to devices and internet connectivity. It includes the ability to use digital tools, locate and evaluate information, communicate effectively, and make informed decisions online. Unequal access to these capabilities can create a digital divide even where smartphones and internet services are available.

Gogoi et al. (2025) examined a digital literacy training programme implemented among adolescent girls in rural Jharkhand between 2017 and 2020. The programme addressed digital access, technical skills, internet use, social media, cybersecurity, and educational opportunities. The authors reported that the proportion of participants scoring above the median digital literacy score was significantly higher in the intervention group than in the comparison group at the midline and endline assessments.

This study provides evidence that structured, context-sensitive digital literacy training can improve digital knowledge and skills in a rural setting. However, its participants were adolescent girls in Jharkhand, and its outcomes were broader than online fraud prevention. Its findings should not be directly generalised to all adult residents of rural Tamil Nadu.

B. Cyber security Awareness and Digital Financial Inclusion

Digital financial inclusion depends not only on the availability of banking services but also on users' willingness and ability to use them safely. Fraud incidents can weaken confidence in online payments and discourage users from adopting digital financial services.

Afzal et al. (2025) investigated cybersecurity awareness, cyber fraud, trust, and payment-banking adoption in rural India. Their study used a model incorporating elements of the Unified Theory of Acceptance and Use of Technology and Diffusion of Innovations theory. The reported findings indicated that cyber fraud negatively affected trust and payment-banking adoption, while cybersecurity awareness, facilitating conditions, and trust were positively associated with adoption.

These findings connect digital safety with the broader goal of financial inclusion. A person who understands the risks of digital transactions and knows how to verify requests may be better equipped to make informed decisions. Nevertheless, awareness does not guarantee protection against sophisticated fraud, and the relationship between knowledge and actual behaviour requires further investigation.

C. Digital Literacy Training in Rural Communities

Training programmes can help participants develop practical skills through demonstrations, guided activities, and locally relevant learning materials. Gogoi et al. (2025) designed a programme that incorporated technical digital skills, cybersecurity, information literacy, and other life skills. The study used repeated assessments and a comparison group to evaluate changes over time.

Its findings support the consideration of culturally appropriate and structured training programmes in rural contexts. They also indicate that digital literacy should be understood as a capability that can be developed rather than as a fixed personal characteristic. However, digital literacy training and fraud-prevention training are not identical. A programme that teaches basic smartphone operation may not sufficiently prepare participants to recognise impersonation attempts, distinguish legitimate communications from deceptive ones, or navigate formal complaint mechanisms.

D. Public Awareness and Consumer Protection

Digital fraud prevention requires cooperation between users, financial institutions, technology providers, public agencies, and community organisations. Individuals need accessible information about safe practices, while institutions need effective systems for responding to complaints and preventing unauthorised transactions.

The Reserve Bank of India's Annual Report 2024–25 documents awareness initiatives relating to safe banking practices, complaint procedures, impersonation fraud, and digital-arrest scams (Reserve Bank of India [RBI], 2025). Such initiatives provide an institutional context for investigating whether rural residents are familiar with available safety information and official reporting channels.

Awareness campaigns may be more useful when they explain specific situations rather than presenting general warnings. For example, participants could be taught to recognise requests for confidential authentication details, verify unexpected payment requests independently, and avoid acting under pressure.

E. Cybersecurity Literacy and Social Inequality

Cybersecurity literacy may vary across individuals because of differences in educational opportunities, digital experience, access to suitable devices, and exposure to reliable information.

Poola et al. (2026) examined cybersecurity literacy and digital vulnerability in India using secondary data from the National Sample Survey's 79th round. The authors reported inequalities in cybersecurity capabilities across demographic and socioeconomic groups.

Their findings reinforce the distinction between access to digital infrastructure and the ability to use it securely.

This national-level evidence is relevant to the proposed rural Tamil Nadu study, but it does not replace local investigation. The circumstances of rural residents may vary according to age, gender, occupation, educational background, and experience with digital financial services. A local survey can help determine which dimensions of digital literacy require greater attention within the selected study communities.

F. Synthesis of the Literature

The reviewed literature suggests three important points. First, digital literacy is broader than device operation and should include security awareness, critical evaluation, and practical decision-making. Second, cybersecurity awareness is relevant to digital financial inclusion because fraud can undermine trust in digital services. Third, structured digital literacy programmes can improve digital skills in rural settings, but the effectiveness of specific interventions for online fraud recognition and reporting should be evaluated directly.

IV. RESEARCH GAP

A. Integration of digital literacy dimensions

Digital literacy includes technical skills, information evaluation, privacy awareness, and the ability to make safe decisions online. Research that focuses primarily on technology adoption may not fully explain how these dimensions relate to practical fraud-recognition capability. The proposed study will examine digital literacy as a set of related capabilities rather than relying exclusively on general self-reported confidence.

B. Local contextual evidence

Research has investigated cybersecurity awareness in rural India, and digital literacy interventions have been evaluated in rural communities elsewhere in the country (Afzal et al., 2025; Gogoi et al., 2025). The proposed study will focus specifically on adult residents of selected rural communities in Tamil Nadu. This geographic focus is a rationale for further investigation, not a claim that no comparable research exists in Tamil Nadu. A comprehensive systematic search will be needed to establish how extensively the precise research question has already been studied.

C. Gap between awareness and practical skills

Knowing that online fraud exists does not necessarily mean that a person can recognise a deceptive payment request or select an appropriate response.

The distinction between awareness, demonstrated recognition, preventive behaviour, and reporting knowledge deserves direct examination. The proposed questionnaire will include scenario-based questions alongside questions about general awareness and reported digital practices.

D. Reporting knowledge

Fraud prevention involves both reducing exposure to suspicious activities and responding appropriately when an incident occurs. Residents may differ in their understanding of how to contact a bank, preserve relevant transaction information, or report a suspected cybercrime. The proposed study will examine reporting knowledge as a separate dimension rather than treating it as equivalent to general cybersecurity awareness.

E. Proposed contribution

The proposed contribution is a context-specific framework linking digital literacy with fraud recognition, preventive practices, and reporting knowledge among adults in rural Tamil Nadu. The study will investigate relationships between these variables rather than presuming that digital literacy automatically reduces fraud incidence. Its findings may inform the design of accessible community-based awareness programmes.

V. AIM AND OBJECTIVES OF THE STUDY

A. Aim

To examine the role of digital literacy in supporting online fraud recognition, prevention, and reporting among adults in rural Tamil Nadu and to propose an evidence-informed framework for community-based digital safety education.

B. Specific objectives

1. To assess digital literacy and cybersecurity awareness among adult residents of selected rural communities in Tamil Nadu.
2. To examine respondents' ability to identify common online fraud scenarios.
3. To assess self-reported digital safety practices, including the protection of confidential information and verification of suspicious requests.
4. To evaluate respondents' awareness of appropriate procedures for reporting suspected online fraud.
5. To examine the association between digital literacy and fraud-recognition capability.

6. To investigate whether educational background, age, digital experience, and previous exposure to awareness programmes are associated with digital safety knowledge and practices.
7. To propose a practical digital literacy framework suitable for rural community awareness initiatives.

VI. RESEARCH QUESTIONS

1. What is the level of digital literacy and cybersecurity awareness among respondents in the selected rural communities?
2. How effectively can respondents identify common online fraud scenarios?
3. What preventive practices do respondents report using when accessing digital financial and communication services?
4. To what extent are respondents familiar with appropriate procedures for reporting suspected online fraud?
5. Is digital literacy associated with the ability to recognise suspicious digital activities?
6. How are educational background, age, digital experience, and exposure to fraud-awareness programmes associated with digital safety knowledge and practices?
7. What components should be included in a community-based digital literacy framework for rural Tamil Nadu?

VII. RESEARCH HYPOTHESES

- H1: Digital literacy is positively associated with online fraud-recognition capability among adult residents of the selected rural communities.
- H2: Cybersecurity awareness is positively associated with self-reported preventive digital practices.
- H3: Exposure to digital safety awareness programmes is associated with higher fraud-recognition scores.
- H4: Digital literacy is positively associated with knowledge of online fraud-reporting procedures.
- H5: The relationship between digital literacy and fraud-recognition capability remains significant after accounting for relevant demographic and digital-access characteristics.

These hypotheses are proposed for statistical testing and are not established findings. H5 is intended for multivariable analysis if the final sample size and data quality are sufficient.

VIII. RESEARCH METHODOLOGY

A. Research design

The study will use a literature review combined with a cross-sectional questionnaire survey. The literature review will establish the conceptual basis, identify relevant constructs, and inform questionnaire development. The survey will collect primary data from adult residents of selected rural communities in Tamil Nadu.

A cross-sectional survey is suitable for describing current awareness and examining associations between variables. However, it cannot establish whether digital literacy causes improved fraud prevention or whether an awareness programme produces lasting behavioural change.

B. Study area

The proposed study area is selected rural communities in Tamil Nadu. Specific districts, blocks, and villages will be selected after assessing feasibility, access, language requirements, and the availability of community-level sampling information. The final proposal should identify the selected locations and explain why they are appropriate for the research question.

C. Target population

The target population will comprise adults aged 18 years and above who reside in the selected rural communities. Eligible participants may include individuals who use smartphones, digital payment services, mobile banking, messaging applications, or other internet-enabled services. To avoid excluding people who have limited digital experience, the survey should also allow participation by residents who have access to digital services but use them infrequently or depend on assistance from others.

D. Sampling technique

A multistage sampling approach is proposed:

Stage 1: Select study districts according to the objectives, feasibility, and availability of rural population information.

Stage 2: Identify eligible villages within selected districts and select them using an appropriate probability-based method where feasible.

Stage 3: Develop or obtain a suitable household sampling frame and select households systematically or randomly.

Stage 4: Select one eligible adult per household using a predefined procedure rather than allowing interviewers to choose the easiest person to contact.

If a complete sampling frame is unavailable, a clearly documented alternative may be required. Convenience sampling should be identified as such and its limitations acknowledged; it should not be described as representative of all rural Tamil Nadu.

E. Proposed sample size

A preliminary target of approximately 384 respondents may be considered for estimating a proportion in a large population under simple random sampling, assuming a 95% confidence level, a 5% margin of error, and an assumed proportion of 50%. This is a planning estimate, not a final sample-size determination.

$$n = Z^2 p(1 - p) / d^2$$

Here, n is the required sample size; $Z = 1.96$ for a 95% confidence level; $p = 0.50$; and $d = 0.05$. The initial estimate does not account for clustering, non-response, finite population size, or the statistical power required to test associations. If villages are sampled as clusters, the sample size should be adjusted using an appropriate design effect and expected response rate.

F. Sources of data

Secondary data will include peer-reviewed journal articles, systematic reviews, official reports, and relevant publications on digital literacy, cybersecurity awareness, online fraud, digital financial inclusion, and fraud reporting. Primary data will be collected through a structured questionnaire administered to eligible adult residents in the selected rural communities.

G. Questionnaire development

The questionnaire will be developed using constructs identified in the literature. It should be available in Tamil and, where appropriate, English. Translation should be reviewed for clarity and conceptual equivalence. The proposed questionnaire will contain the following sections:

TABLE I
PROPOSED QUESTIONNAIRE

Section	Variables to be measured
A. Demographic information	Age group, gender, education, occupation, and relevant background characteristics
B. Digital access and use	Device access, internet access, frequency of use, and use of digital financial services
C. Digital literacy	Ability to use digital services, evaluate information, and understand basic digital

	functions
D. Cybersecurity awareness	Knowledge of suspicious links, impersonation, requests for confidential details, and fraudulent payment requests
E. Fraud recognition	Responses to hypothetical online fraud scenarios
F. Preventive practices	Verification habits, protection of confidential information, and response to unexpected requests
G. Reporting knowledge	Awareness of suitable bank contacts and official cybercrime reporting channels
H. Training exposure	Previous participation in digital literacy or fraud-awareness programmes

H. Pilot testing and validity

Before the main survey, the questionnaire will be reviewed by subject experts in digital literacy, cybersecurity, social science research, and survey methodology. A small pilot study should be conducted with eligible individuals who are not included in the main survey, where practicable. The pilot will assess comprehension, translation quality, interview duration, response options, and questions that participants find confusing or uncomfortable.

Content validity can be assessed through expert review. Internal consistency measures, such as Cronbach's alpha, may be appropriate for multi-item scales intended to measure a common construct. Such measures should not automatically be applied to factual knowledge questions that assess different skills. The final questionnaire and scoring rules should be established before full data collection.

I. Operationalization of variables

TABLE II
Operationalization of variables

Variable	Proposed measurement
Digital literacy	Score based on specified digital knowledge and practical skill questions
Cybersecurity awareness	Number or proportion of relevant safety questions answered correctly
Fraud-recognition capability	Correct identification of safe and unsafe responses to hypothetical scenarios

Preventive practices	Responses concerning reported safety behaviours
Reporting knowledge	Correct identification of appropriate actions and reporting channels
Training exposure	Previous participation in digital literacy or cybersecurity awareness programmes
Background characteristics	Demographic, educational, and digital-access variables

A scoring rubric will be prepared before analysis. For scenario-based questions, the expected safe response should be established using reliable official guidance. Where a measure has not been validated for the study population, it should be described as a study-developed measure rather than a validated scale.

J. Data collection procedure

After obtaining institutional approval and any required local permissions, trained data collectors will approach eligible residents and explain the purpose of the research. Participants will receive an information sheet in an accessible language and will be informed that participation is voluntary. Consent will be obtained before administering the questionnaire.

Data may be collected through paper questionnaires or secure electronic forms, depending on local access and participant preference. For participants with limited reading ability, trained interviewers may read questions aloud in a neutral manner. The questionnaire will use hypothetical examples rather than asking participants to disclose bank credentials, one-time passwords, account numbers, or unnecessary details of actual financial transactions.

K. Proposed data analysis

Descriptive statistics: Frequencies, percentages, means, standard deviations, medians, and interquartile ranges will be used as appropriate to summarise respondent characteristics and digital literacy measures.

Score construction: Predefined scoring rules will be used to calculate digital literacy, cybersecurity awareness, and fraud-recognition scores. Missing responses will be handled using a documented rule rather than automatically treating them as incorrect.

Bivariate analysis: Chi-square tests may be used to examine associations between categorical variables. Correlation tests may be used to examine relationships between suitable continuous or ordinal measures. Pearson or Spearman correlation will be selected according to measurement properties and distributional assumptions.

Multivariable analysis: If supported by sample size and data structure, regression models may examine whether digital literacy is associated with fraud-recognition capability after adjustment for relevant background characteristics.

Statistical significance: A significance level of .05 may be specified in advance, alongside effect sizes and confidence intervals. Statistical significance alone should not be interpreted as evidence of practical importance or causation.

No statistical results are presented in this proposal because primary data have not yet been collected.

L. Ethical considerations

- Obtain ethics approval before recruitment if required by the institution.
- Explain the purpose, procedures, risks, and voluntary nature of participation.
- Obtain informed consent from all participants.
- Avoid collecting unnecessary personally identifiable or financial information.
- Store research data securely and restrict access to authorised researchers.
- Allow participants to decline questions or withdraw in accordance with the approved protocol.
- Report results in aggregate form and avoid identifying individuals or households.
- Provide accurate, non-alarmist safety information where appropriate.

If a participant discloses a recent fraud incident, the researcher should not promise recovery of lost money or provide unverified advice. Any information about reporting procedures should come from current official sources.

IX. PROPOSED CONCEPTUAL FRAMEWORK

The proposed framework links digital literacy with the capability to recognise, prevent, and report online fraud. It draws on the literature concerning cybersecurity awareness and digital financial inclusion (Afzal et al., 2025), digital literacy training in rural communities (Gogoi et al., 2025), and cybersecurity inequalities (Poola et al., 2026).

1. *Digital literacy:* technical skills, information evaluation, and privacy awareness.

2. *Cybersecurity awareness and practical skills:* fraud recognition, verification habits, and safe digital behaviour.
3. *Fraud-prevention capability:* identifying suspicious requests, avoiding unsafe actions, and protecting information.
4. *Reporting knowledge and response readiness:* knowing whom to contact, understanding reporting procedures, and responding promptly.
5. *Contextual factors:* age, education, digital access, previous training, language, and access to support.



Figure 1. Proposed conceptual framework for the study

The relationships are to be investigated and should not be interpreted as established causal effects.

The framework proposes that digital literacy may support cybersecurity awareness and practical decision-making. These capabilities may be associated with safer digital practices and greater knowledge of reporting procedures. Fraud prevention also depends on factors beyond individual knowledge: fraudsters may use sophisticated techniques, and even digitally skilled users can become victims. Effective prevention therefore requires both individual capabilities and accessible institutional support.

X. PROPOSED DIGITAL LITERACY INTERVENTION

Based on the literature, the study may inform the development of a community-based digital safety programme. The programme is proposed as a potential application of the research, not as an intervention already conducted.

TABLE III

Module	Content	Intended learning outcome
1. Digital basics	Safe use of smartphones, applications, and online services	Understand basic digital operations
2. Recognising fraud	Common phishing, impersonation, and deceptive payment scenarios	Identify warning signs
3. Protecting information	Password safety, authentication details, suspicious links, and privacy	Apply basic protective practices
4. Safe digital payments	Verifying recipients, payment requests, and transaction details	Make informed transaction decisions
5. Reporting and response	Contacting banks and using official cybercrime reporting channels	Identify appropriate response procedures
6. Practical assessment	Hypothetical scenarios, demonstrations, and feedback	Demonstrate and reinforce learning

Training materials should be developed in accessible Tamil, use familiar examples, and accommodate participants with limited reading ability. Sessions could be delivered through community centres or other locally appropriate venues in collaboration with trained facilitators.

If an intervention is subsequently implemented, its effectiveness should be evaluated rather than assumed. A pre-test and post-test design with a comparison group, where feasible, would provide stronger evidence than participant satisfaction alone.

XI. EXPECTED OUTCOMES

Because this is a proposal, the following are anticipated contributions rather than actual research findings.

1. A profile of digital literacy: the study may identify areas in which respondents have stronger or weaker digital knowledge and practical skills.
2. An assessment of fraud awareness: scenario-based questions may reveal which common warning signs are understood and which require further explanation.
3. Evidence about preventive practices: the survey may clarify the relationship between cybersecurity awareness and self-reported digital safety behaviour.

4. An assessment of reporting knowledge: the study may identify gaps in familiarity with official reporting channels and appropriate responses.
5. A context-specific framework: findings may inform the development of digital safety education suitable for selected rural communities in Tamil Nadu.
6. Recommendations for future intervention research: results may help researchers design and evaluate structured digital literacy programmes.

These outcomes will depend on the quality of sampling, questionnaire design, data collection, and analysis. No particular result or direction of association can be guaranteed.

XII. IMPLICATIONS OF THE STUDY

A. Implications for rural communities

The study may help community organisations identify practical digital safety topics that require greater attention. Awareness initiatives can focus on understandable examples, safe transaction habits, and the importance of independently verifying unexpected requests.

B. Implications for educational institutions

Schools, colleges, adult education programmes, and community learning centres may use the eventual findings to develop workshops on digital literacy and cybersecurity. Such programmes should combine general awareness with opportunities to practise identifying suspicious scenarios.

C. Implications for policymakers

The findings may provide local evidence to inform the design of accessible digital inclusion programmes. Particular emphasis could be placed on language accessibility, practical security skills, and knowledge of official reporting mechanisms.

D. Implications for financial institutions

Banks and digital payment service providers may benefit from understanding which fraud warnings are difficult for rural users to interpret. The study could inform the design of clearer customer communications and targeted awareness materials.

E. Implications for future researchers

The proposed framework may support further research examining whether digital literacy is associated with fraud-recognition capability, whether educational interventions improve practical skills, and whether those improvements persist over time.

XIII. LIMITATIONS OF THE PROPOSED STUDY

Geographical scope: The proposed study will cover selected rural communities rather than all of Tamil Nadu. Findings may not be generalisable to every rural population.

Cross-sectional design: A one-time survey can identify associations but cannot establish causal relationships or determine whether digital literacy reduces actual fraud incidence.

Self-reported behaviour: Respondents may overestimate their safety practices or have difficulty recalling previous experiences. Scenario-based questions can complement self-reports but cannot fully reproduce real-world fraud encounters.

Sampling limitations: The quality of findings will depend on the sampling frame, recruitment procedures, response rate, and representation of relevant demographic groups.

Measurement limitations: Study-developed digital literacy and fraud-recognition questions will require careful review and pilot testing. They should not be described as validated measures unless appropriate validation has been conducted.

Sensitive information: Fraud experiences and financial losses may be distressing or private. The questionnaire should minimise unnecessary disclosure and protect participants' confidentiality.

Changing fraud techniques: Online fraud methods evolve. The questionnaire and awareness materials should be reviewed against current official guidance before use.

No current empirical results: Primary data have not yet been collected. The paper cannot establish the actual level of digital literacy among rural residents, test the hypotheses, or claim that the proposed framework has been validated.

XIV. CONCLUSION

Digital literacy is an important capability for safe and informed participation in an increasingly digital society. For rural communities, the ability to access digital services must be accompanied by the skills needed to evaluate information, recognise suspicious activities, protect confidential information, and respond appropriately to suspected online fraud.

Existing research has examined the relationship between cybersecurity awareness and digital financial inclusion in rural India, while intervention research has demonstrated that structured digital literacy training can improve digital skills in rural settings (Afzal et al., 2025; Gogoi et al., 2025).

These findings provide a basis for investigating the relationship between digital literacy and fraud-prevention capability among adult residents of rural Tamil Nadu.

The proposed study will address this issue through a literature review and a questionnaire survey. It will examine digital literacy, cybersecurity awareness, fraud-recognition capability, preventive practices, and reporting knowledge. A conceptual framework will guide the investigation and help organise the relationships among these constructs.

The proposed research does not assume that digital literacy alone can eliminate online fraud. Rather, it treats literacy as one component of a broader approach that also includes institutional safeguards, accessible reporting procedures, responsible technology design, and community awareness.

Ultimately, the study aims to provide an evidence-informed foundation for developing practical, locally accessible digital safety education. Its value will depend on transparent methodology, careful analysis, and recommendations grounded in the data actually collected.

REFERENCES

- [1] Afzal, M., Meraj, M., Kaur, M., & Ansari, M. S. (2025). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario? *Journal of Cyber Security Technology*, 9(2), 88–126. <https://doi.org/10.1080/23742917.2024.2347674>
- [2] Gogoi, A., Manoranjini, M., & Gupta, M. (2025). Design and implementation of digital literacy training programme: Findings of a quasi-experimental study from rural India. *PLOS Digital Health*, 4(4), e0000617. <https://doi.org/10.1371/journal.pdig.0000617>
- [3] Poola, D., Chakradhar, J., Kasarapu, S. S. K., et al. (2026). Mapping cybersecurity literacy: Inequality, capability, and digital vulnerability in India. *Humanities and Social Sciences Communications*. <https://doi.org/10.1057/s41599-026-08409-z>
- [4] Reserve Bank of India. (2025). Annual report 2024–25. <https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx>
- [5] International Telecommunication Union. (2024). Digital skills toolkit. https://www.itu.int/hub/publication/d-phcb-cap_develop-01-2024/
- [6] Law, N., Woo, D., de la Torre, J., & Wong, G. (2018). A global framework of reference on digital literacy skills for indicator 4.4.2. UNESCO Institute for Statistics. <https://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf>
- [7] Organisation for Economic Co-operation and Development. (2015). Digital security risk management for economic and social prosperity. OECD Publishing. <https://doi.org/10.1787/9789264245471-en>
- [8] Government of India. (n.d.). National Cyber Crime Reporting Portal. <https://www.cybercrime.gov.in/>
- [9] Indian Computer Emergency Response Team. (n.d.). Cyber security awareness and guidance for citizens. <https://www.cert-in.org.in/>
- [10] Ministry of Home Affairs, Government of India. (n.d.). Indian Cyber Crime Coordination Centre (I4C). <https://i4c.mha.gov.in/>