ASEAN Journal of
Community Service and Education

Journal homepage: https://ejournal.bumipublikasinusantara.id/index.php/ajcse

Community-Based Artificial Intelligence (AI) Empowerment for Rural Girls: A Theoretical Framework for Digital Literacy, Cybersecurity, and Sustainable Community Development

*Ritesh Karmaker**

Nizam Uddin Ahmed Model College, Mymensingh, Sherpur, Bangladesh
*Correspondence: E-mail: karmakerritesh@gmail.com

ABSTRACT

This study develops a community-based Artificial Intelligence (AI) empowerment framework for rural girls in Bangladesh by integrating digital literacy, cybersecurity, and sustainable community development. A quantitative survey involving 1,006 participants was supported by stakeholder consultations with 37 educators, researchers, and community actors. Rural girls face limited digital access, high mobile data costs, online fraud, privacy risks, and inaccurate AI information. The framework positions security-conscious agency as the mechanism through which digital access, AI skills, and community support produce sustainable empowerment. It also highlights the role of schools, families, local institutions, and community service programs in strengthening safe AI participation. The study offers a practical model for inclusive digital education, protective literacy, and community-based interventions in resource-constrained rural communities.

ARTICLE INFO

Article History:
Submitted/Received 08 Mar 2026
First Revised 25 Jun 2026
Accepted 30 Jul 2026
First Available online 02 Aug 2026
Publication Date 01 Sep 2027

Keyword:
Artificial intelligence;
Community empowerment;
Community service;
Cybersecurity;
Digital literacy.

1. INTRODUCTION

Artificial intelligence (AI) is increasingly used to support learning, information access, communication, creativity, and problem-solving across educational and community contexts (Nnanguma, 2025; Jimoh *et al.*, 2027; Abosede *et al.*, 2025; Amado and Digo, 2026; Katel, 2026; Davidson *et al.*, 2026). However, the educational benefits of AI are not distributed equally. Rural communities in developing countries often experience limited internet connectivity, inadequate access to digital devices, high mobile data costs, and insufficient opportunities for structured digital training. These constraints are particularly serious for rural girls, who may also face gender-based restrictions, limited family support, and greater exposure to online harassment, fraud, privacy violations, and misleading information.

Traditional technology-adoption theories explain digital participation mainly through perceived usefulness, ease of use, social influence, and facilitating conditions (Davis, 1989; Venkatesh *et al.*, 2003). These concepts remain important, but they do not fully explain technology use in communities where participation itself may create social, financial, or personal risks. Rural girls may have access to smartphones or AI applications but still avoid independent use because they fear online scams, identity misuse, inaccurate AI-generated information, or inappropriate exposure of personal data.

Digital empowerment must therefore extend beyond device ownership and internet connectivity. Meaningful empowerment requires the ability to use digital technologies safely, critically, confidently, and independently. Human-centered AI emphasizes that AI systems should be reliable, safe, trustworthy, and responsive to human needs (Shneiderman, 2020). Similarly, sociotechnical perspectives explain that technological outcomes depend on interactions among infrastructure, users, institutions, and social environments (Baxter and Sommerville, 2011). These perspectives indicate that AI empowerment cannot be achieved through technology provision alone.

Community-service initiatives can connect educational expertise with local needs through training, mentoring, technology-supported learning, and institutional collaboration (Abosede *et al.*, 2025; Bolaji *et al.*, 2025). In rural settings, schools, colleges, universities, local authorities, families, nongovernmental organizations, and community groups can work together to provide AI literacy, cybersecurity education, mentoring, and locally relevant digital support. Community-based programs can reduce the distance between formal education and the everyday digital needs of rural girls. They can also ensure that participants receive assistance from trusted institutions and community members.

Community involvement is especially important because digital participation is shaped by social relationships. Families may encourage or restrict technology use, peers may influence confidence and behaviour, and educational institutions may provide safe learning environments. Community service programs can strengthen these enabling relationships while addressing misinformation, online fraud, data privacy, and responsible AI use. Consequently, community-based AI education should combine technological access, skill development, social support, and cybersecurity awareness.

Previous research in Bangladesh has shown that digital literacy can strengthen educational participation among rural women, but regional disparities, infrastructural limitations, and gender inequalities continue to restrict meaningful digital inclusion (Karmaker and Cvetković, 2025). The original findings of the present study similarly indicate differences in access, participation, and safety awareness among rural students. Rural girls face not only economic

and infrastructural barriers but also uncertainty about whether AI information can be trusted and whether digital environments are secure.

The Community-Based Rural Girls' Artificial Intelligence Empowerment Framework explains how digital access, AI engagement and skill development, cybersecurity awareness, and community support contribute to sustainable empowerment. Within the framework, security-conscious agency functions as the central mechanism that enables rural girls to use AI safely, critically, and independently. Community-based support provides the practical pathway through which schools, families, educators, local institutions, and community organizations can strengthen digital literacy, reduce cybersecurity risks, and promote meaningful and sustainable AI participation.

As a continuation of previous studies (Karmaker, 2025a; Karmaker, 2025b; Karmaker, 2026), this study aims to develop and examine a community-based AI empowerment framework for rural girls in Bangladesh. Specifically, it investigates how digital access, AI engagement, cybersecurity awareness, and community support influence sustainable empowerment. It also considers how community service programs can translate these dimensions into practical interventions for digital literacy, protective education, and inclusive rural development.

The novelty of this study lies in integrating community service, AI education, cybersecurity, and sustainable community development within one framework. Previous technology-adoption models have mainly emphasized user acceptance, while digital-empowerment studies have generally focused on access and skills. The present study positions security-conscious agency as a central mechanism and interprets community support as an active educational and developmental intervention. The framework therefore provides a practical basis for designing community-based AI literacy programs for rural girls in resource-constrained settings.

Previous research has established the importance of technology acceptance, digital access, human-centered design, and sociotechnical interaction (Davis, 1989; Venkatesh *et al.*, 2003; Baxter and Sommerville, 2011; Shneiderman, 2020). Research in Bangladesh has also demonstrated the relationship between digital literacy and educational empowerment among rural women (Karmaker and Cvetković, 2025). Nevertheless, three gaps remain. First, existing models commonly treat cybersecurity as an external concern rather than as a central condition of empowerment. Second, many studies discuss community support as a contextual factor but do not translate it into structured community service interventions. Third, limited research integrates AI literacy, cybersecurity, gender inclusion, and sustainable rural development within a single framework.

The present study addresses these gaps through a community-based AI empowerment framework. The framework links digital access, AI engagement and skill development, awareness, and community support with security-conscious agency. Sustainable individual and community empowerment emerges when participants can convert available technological resources into safe, meaningful, and independent outcomes.

2. LITERATURE REVIEW

As summarized in **Table 1**, previous studies provide important foundations for understanding technology adoption, digital literacy, and safe AI. However, they do not fully explain how community service can combine these dimensions to produce sustainable

empowerment among rural girls. The present study fills this gap by positioning security-conscious agency as the central mechanism and community-based support as the practical foundation of intervention.

Table 1. Synthesis of previous studies and the research gap.

REFERENCE	MAIN FOCUS	CONTRIBUTION	LIMITATION ADDRESSED BY THIS STUDY
Davis (1989)	Technology acceptance	Explains adoption through usefulness and ease of use	Does not place cybersecurity or community service at the center of empowerment
Venkatesh *et al.* (2003)	Unified technology adoption	Includes social influence and facilitating conditions	Focuses more on adoption than safe and sustainable empowerment
Baxter and Sommerville (2011)	Sociotechnical systems	Connects technology with social and institutional environments	Does not provide a specific community-service model for rural girls
Shneiderman (2020)	Human-centered AI	Emphasizes reliable, safe, and trustworthy AI	Focuses mainly on system design rather than community-level protective agency
Karmaker and Cvetković (2025)	Rural women's digital literacy in Bangladesh	Shows that digital literacy supports educational empowerment	Does not fully integrate cybersecurity, AI literacy, and community service
Present study	Community-based AI empowerment	Integrates access, AI skills, cybersecurity, community support, and sustainable development	Provides a framework for practical community-service interventions

2.1. Artificial Intelligence and Rural Digital Inequality

AI technologies can support educational participation by providing access to information, personalized learning, language assistance, academic writing support, and digital communication. Nevertheless, students cannot benefit equally when internet infrastructure, devices, training opportunities, and social support remain unevenly distributed.

The rural-urban digital divide includes differences in connectivity, affordability, digital skills, institutional support, and opportunities for meaningful use. Rural students may technically have access to mobile phones while still experiencing weak networks, expensive mobile data, shared devices, and limited digital guidance. Therefore, access should not be defined only as device ownership. It should include the reliability, affordability, safety, and educational usefulness of digital technology.

Digital literacy contributed to educational empowerment among rural women in Bangladesh, but structural barriers and regional inequalities continued to limit participation (Karmaker and Cvetković, 2025). Digital inclusion requires both technological investment and educational intervention. Infrastructure may create opportunities, but users also need relevant skills and confidence to convert access into meaningful outcomes.

The challenge is particularly important for rural girls. Gendered expectations may influence when, where, and how digital devices are used. Families may restrict technology use because of concerns about online safety, social reputation, or inappropriate content. These concerns cannot be dismissed as resistance to technology because many are connected to real risks, including fraud, harassment, privacy breaches, and misinformation.

2.2. Technology Acceptance and Its Limitations

The Technology Acceptance Model explains technology use through perceived usefulness and perceived ease of use (Davis, 1989). The Unified Theory of Acceptance and Use of Technology expands this explanation by incorporating performance expectancy, effort expectancy, social influence, and facilitating conditions (Venkatesh *et al.*, 2003). These models have been widely used to study technology adoption in organizational and educational environments. However, technology acceptance does not necessarily produce empowerment. A student may consider AI useful and easy to use but still cannot verify inaccurate information, protect personal data, identify scams, or make independent decisions. Technology adoption models also commonly assume relatively stable environments in which risks are manageable through organizational systems.

Rural digital environments may differ from these assumptions. Participants may access AI through personal or shared mobile devices without formal supervision, institutional cybersecurity systems, or immediate technical assistance. Under such conditions, willingness to use technology is only one part of the empowerment process. Users must also possess protective knowledge and critical judgement.

The present framework therefore moves from adoption toward sustainable empowerment. Adoption refers to whether individuals use technology, whereas empowerment refers to whether they can use it safely, independently, critically, and productively. This distinction is essential for community service because training programs should not merely increase AI usage. They should also strengthen informed decision-making and responsible digital behaviour.

2.3. Human-Centered AI and Protective Digital Literacy

Human-centered AI emphasizes the development of reliable, safe, trustworthy, and inclusive systems that support human goals (Shneiderman, 2020). This perspective is relevant to rural community development because AI tools should be understandable, accessible, and appropriate for users with different levels of digital experience.

However, safe system design alone cannot eliminate all user-level risks. Rural girls may use commercially available AI platforms that were not designed specifically for their linguistic, educational, or cultural contexts. They may encounter inaccurate information, biased responses, privacy concerns, and unclear data-use practices. Therefore, human-centered AI must be supported by protective digital literacy.

Protective digital literacy includes the ability to recognize fraud, evaluate AI-generated information, protect personal information, understand privacy risks, and use digital tools responsibly. Within the proposed framework, these abilities form part of security-conscious agency. This agency allows participants to make informed decisions before accepting information or sharing personal data.

Community service programs can strengthen protective literacy through demonstrations, workshops, mentoring, peer education, and scenario-based training. For example, participants can learn how to identify suspicious links, verify AI-generated academic content, create stronger passwords, and avoid sharing sensitive images or personal information. These activities transform cybersecurity from an abstract technical topic into practical community education.

2.4. Sociotechnical Systems and Community Context

Sociotechnical theory explains that technological systems cannot be separated from their social and institutional environments. Technology, people, organizational arrangements, and social practices influence one another (Baxter and Sommerville, 2011). In rural AI education, the effectiveness of technology depends on infrastructure, family attitudes, teacher support, local institutions, economic conditions, and community trust.

Providing devices without training may produce limited educational benefits. Similarly, providing training without affordable connectivity may prevent continued participation. Community-based AI empowerment therefore requires coordination among technological and social components.

Schools and colleges can provide structured learning spaces. Teachers can guide responsible use. Families can encourage safe participation. Local government and nongovernmental organizations can support infrastructure and training. Peer networks can provide practical assistance and reduce fear. Through collaboration, these actors can create a supportive sociotechnical environment.

This perspective also explains why community service should not be designed as a one-time activity. Sustainable empowerment requires continued support, feedback, mentoring, and adaptation. Community members should participate in identifying local needs, selecting training topics, and evaluating program outcomes. Such participation can increase relevance, trust, and long-term engagement.

2.5. Security-Conscious Agency

Security-conscious agency refers to the ability to participate in digital environments while recognizing risks, evaluating information, protecting personal data, and making independent decisions. It combines awareness, critical literacy, confidence, and responsible behaviour.

In the proposed framework, security-conscious agency functions as the mechanism through which access and skills are converted into sustainable empowerment. Without this mechanism, improved connectivity may increase exposure to cyber risks rather than produce meaningful development. Similarly, AI training that focuses only on operational skills may leave participants unable to recognize misinformation or privacy threats.

The framework addresses concerns related to financial fraud, online scams, inaccurate AI-generated information, data privacy, and responsible AI use. Rural girls evaluate AI not only according to its usefulness but also according to whether its use is safe and trustworthy.

Community service interventions should therefore integrate cybersecurity with AI literacy. Digital safety should not be presented as a separate or optional topic after technical training. It should be included throughout the learning process. Every lesson on AI use should also address verification, privacy, ethics, and risk.

2.6. Community Support and Social Capital

Community support includes encouragement, guidance, trust, peer networks, institutional assistance, and access to local role models. These resources can increase confidence and reduce uncertainty among new technology users.

In rural communities, family attitudes may strongly influence girls' digital participation. Supportive families may allow girls to attend training, use devices, and explore educational applications. Conversely, fear of online harm may lead families to restrict digital access. Community-based cybersecurity education can help families understand both the benefits and risks of AI, enabling them to support safer participation rather than prohibiting technology use entirely.

Peer networks can also support learning. Participants may share information, explain applications, discuss risks, and help one another solve technical problems. Educators and local female role models can demonstrate that AI skills are relevant to education, employment, entrepreneurship, and community leadership.

Community service programs can organize these relationships into structured support systems. Activities may include AI literacy workshops, cybersecurity campaigns, peer mentoring, family information sessions, community technology centers, and collaboration between educational institutions and local organizations.

2.7. Community Service and Sustainable Development

Community service connects educational knowledge with social needs. Universities, colleges, and schools can apply their expertise through training, mentoring, outreach, and community partnerships. In the context of AI empowerment, community service can translate digital knowledge into practical programs for underserved rural populations.

Sustainable community development requires more than short-term technology distribution. Programs should strengthen local knowledge, confidence, institutional capacity, and continued access to support. They should also reduce inequalities rather than create new forms of dependency.

AI empowerment can contribute to sustainable development by improving educational participation, access to information, employment readiness, entrepreneurship, and social inclusion. However, these outcomes depend on whether participants can use AI safely and critically. Cybersecurity is therefore part of sustainability because unsafe participation may lead to financial loss, privacy violations, mistrust, and withdrawal from digital environments.

Community-based programs should be participatory, context-sensitive, and inclusive. Rural girls should not be treated only as recipients of training. Their experiences, concerns, and aspirations should guide program design. This approach strengthens ownership and ensures that intervention goals remain relevant to local needs.

3. METHODS

This study employed a quantitative survey design supported by supplementary stakeholder consultations to examine how digital access, AI engagement, cybersecurity awareness, and community support were associated with the empowerment of rural girls in Bangladesh. The quantitative survey provided evidence concerning digital access, safety awareness, socioeconomic barriers, and empowerment outcomes, while the stakeholder consultations supplied contextual information for interpreting the statistical findings and developing community-service recommendations.

The research was conducted in Sherpur Sadar Upazila, Bangladesh, between January 19, 2023, and February 9, 2026, following an initial pilot-testing period. The principal target

population consisted of rural female students aged 18–26 years who had completed at least secondary education and had lived in Sherpur Sadar Upazila for a minimum of 12 months.

The quantitative survey involved 1,006 participants recruited through non-probability convenience sampling. The final sample included 984 female and 22 male respondents. 887 lived in rural areas, and 119 lived in urban areas. Because the sample was predominantly female and rural, the findings were interpreted primarily in relation to rural girls, while the minority groups were retained to preserve the completeness of the dataset.

Supplementary stakeholder consultations involved 37 participants selected through purposive sampling based on their experience in education, AI, digital technology, women's empowerment, or community development. Of these participants, 26 joined focus group discussions, six provided written structured responses, and five participated in individual interviews. The consultations explored digital access, cybersecurity risks, AI literacy, community support, training needs, and the potential roles of educational institutions and community-service organizations.

The quantitative instrument consisted of 11 Likert-scale items. Items Q1–Q4 measured security-conscious agency, including awareness of digital-safety risks, financial fraud, inaccurate AI information, data privacy, and responsible AI use. Items Q5–Q7 measured digital access and socioeconomic barriers, including device availability, mobile data costs, and the need for AI-safety training. Items Q8–Q11 measured empowerment and agency outcomes, including social recognition, self-presentation, global academic participation, and economic-independence potential.

Before the main survey was administered, the instrument was pilot-tested with 60 students who had characteristics similar to those of the target participants. These students were excluded from the final sample. The instrument produced a Cronbach's alpha of 0.87, indicating satisfactory internal consistency.

Questionnaires were administered both online and in person to accommodate participants with different levels of internet connectivity. In-person questionnaires were completed in controlled group settings. Focus group discussions and individual interviews were conducted in a computer-training centre equipped with comparable computer systems. Participants were assured that their responses would remain anonymous, and institutional supervisors were not involved during questionnaire completion.

Quantitative data were processed using Microsoft Excel 365. Frequencies, percentages, means, and standard deviations were calculated to describe participant characteristics and questionnaire responses. Multiple linear regression was used to examine associations between seven selected indicators and AI-empowerment outcomes. Because the predictors were individual questionnaire items rather than validated latent constructs, the regression coefficients were interpreted as item-level associations and not as statistical validation of the complete framework or its proposed mediating mechanism.

Stakeholder responses from focus group discussions, written structured responses, and individual interviews were reviewed thematically (Braun and Clarke, 2006). The review identified recurring contextual issues related to digital access, misinformation, privacy, fraud, family encouragement, peer support, institutional responsibility, and training needs. These contextual observations were used to support the interpretation of the quantitative findings

and to formulate the proposed community-service model. They were not analysed as an independent qualitative dataset or presented as separate thematic findings.

Questionnaires containing more than 10% missing data were excluded. For minor missing values below 5%, mean substitution was applied. Responses were also examined for logical inconsistencies involving age, residence, and educational level.

Ethical approval was granted under Approval No. NAMC/01-02-24.00.04.00044. All participants provided written informed consent. Participation was voluntary, and personal identifiers were removed from the dataset.

4. RESULTS AND DISCUSSION

The quantitative findings show that AI empowerment among the predominantly rural female sample was associated with digital access, cybersecurity awareness, socioeconomic barriers, and empowerment aspirations. The statistical results are presented through participant characteristics, descriptive indicator scores, dimensional analysis, and multiple regression. Stakeholder consultations are used as contextual support for interpreting these findings and developing the community-service implications presented in the later sections.

Figure 1 presents the conceptual Community-Based Rural Girls' Artificial Intelligence Empowerment Framework derived from the literature, survey indicators, statistical findings, and contextual stakeholder consultations. The framework proposes that sustainable empowerment may emerge through the interaction of digital access, AI engagement and skill development, and community-based support. Security-conscious agency is positioned as a central conceptual mechanism that includes cognitive awareness of risk and critical AI literacy. The rural–urban divide and social exclusion operate as external pressures, while community-based support provides a feedback pathway that may strengthen continued participation, digital confidence, and sustainable community development.

The framework positions security-conscious agency as a theoretically proposed mechanism rather than an empirically confirmed mediator. Digital access and AI skills may not automatically produce empowerment unless participants can recognize fraud, evaluate inaccurate information, protect personal data, and use AI responsibly. Community-based support links these individual capabilities with broader participation by involving families, educators, peers, local institutions, and community organizations.

4.1. Participant Characteristics and Community Context

Table 2 presents the socio-demographic characteristics of the 1,006 survey participants. The sample was predominantly female and rural. Female participants represented 97.81% of the sample, while 88.17% lived in rural communities. Most respondents were aged 18–20 years, indicating that the findings primarily reflect young women transitioning from secondary education to higher education or employment.

The educational profile also has implications for community service. More than half of the participants held a Higher Secondary Certificate or equivalent qualification, while a substantial proportion had entered honours-level education. Community-based AI programs should therefore build on participants' existing academic experience while addressing specific gaps in AI literacy, cybersecurity, information verification, and responsible digital participation.

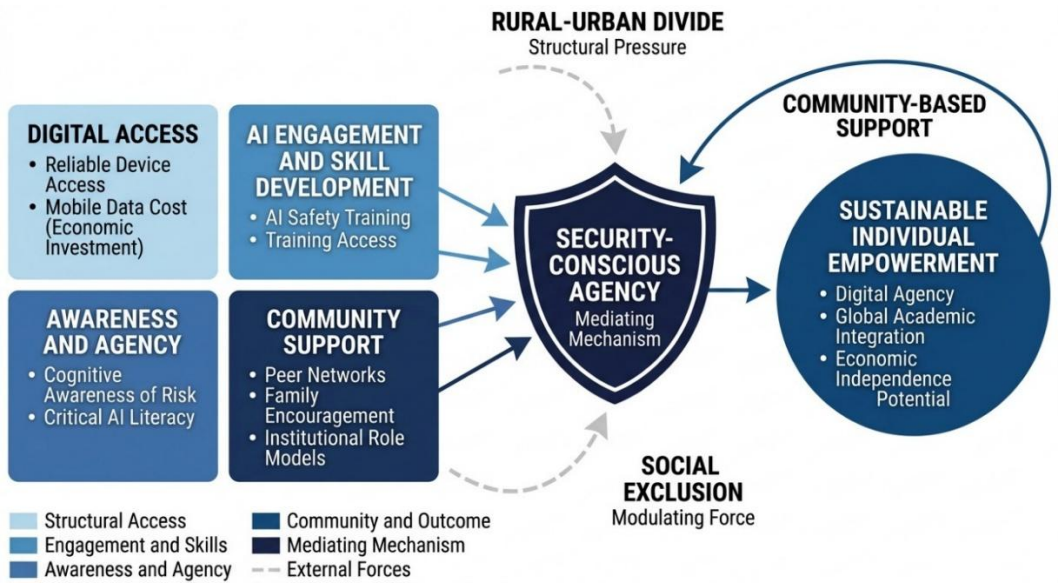

Figure 1. Community-based rural girls' artificial intelligence empowerment framework.

Table 2. Socio-demographic characteristics of participants.

CHARACTERISTIC	CATEGORY	FREQUENCY	PERCENTAGE (%)
Age	18–20 years	938	93.24
	21–23 years	60	5.96
	24–26 years	8	0.80
Gender	Female	984	97.81
	Male	22	2.19
Highest educational qualification	Higher Secondary Certificate/Grade 12	537	53.38
	BA pass	128	12.72
	BSc	20	1.99
	BA	12	1.19
	Honours, all years	294	29.22
	MA	11	1.09
	Secondary School Certificate	4	0.40
Residence	Urban	119	11.83
	Rural	887	88.17
Marital status	Married	267	26.54
	Unmarried	739	73.46

The inclusion of 119 urban participants provides limited comparative context. However, because the dataset was not balanced for a formal rural-urban comparison, the findings should primarily be interpreted in relation to the predominantly rural participant group.

4.2. Digital Safety, Access, and Empowerment Indicators

Table 3 presents the means and standard deviations of the 11 framework indicators. Based on the response coding used in the survey, lower mean scores indicate stronger agreement. Under this interpretation, participants expressed particularly strong agreement regarding the importance of global academic standards, digital-safety risks, inaccurate AI information, and data privacy.

Table 3. Mean and standard deviation of community-based AI-empowerment indicators.

CODE	INDICATOR	MEAN	SD
Q1	Recognition of digital-safety risks, including image misuse and online traps	1.14	0.57
Q2	Perception of financial fraud and online scams as barriers	1.77	0.87
Q3	Critical evaluation of inaccurate AI-generated information	1.27	0.63
Q4	Prioritization of data privacy and responsible AI use	1.29	0.59
Q5	Reliable access to a personal smartphone or computer	2.03	0.93
Q6	Mobile data cost as a financial burden	1.69	0.52
Q7	Perceived need for specialized AI-safety training	1.45	0.50
Q8	Perceived social prestige associated with AI use	1.95	0.63
Q9	AI use for personal empowerment and self-presentation	2.21	1.08
Q10	AI use for meeting global academic standards	1.11	0.47
Q11	Perceived potential of AI for economic independence	1.62	0.84

Q10 produced the lowest mean score (M = 1.11, SD = 0.47), indicating strong recognition of AI as a tool for maintaining global academic competitiveness. However, Q1, Q3, and Q4 also produced low mean scores. These results show that participants' interest in AI was accompanied by substantial concern about image misuse, inaccurate information, privacy, and ethical use. This combination supports a safety-first approach to community service. Community programs should not encourage wider AI use without simultaneously teaching information verification, privacy protection, ethical prompting, image safety, account security, and responsible academic use. Q9 had the highest mean and largest standard deviation (M = 2.21, SD = 1.08). This result indicates considerable variation in how participants viewed AI as a tool for personal empowerment or self-presentation. The variation may reflect differences in confidence, family attitudes, online exposure, educational level, or perceived social risk. Community-based programs should therefore avoid assuming that all participants have the same needs or prior digital experience. Reliable device access also showed considerable variation (Q5: M = 2.03, SD = 0.93). Training programs based entirely on individual device ownership could exclude disadvantaged participants. Shared laboratories, school-based computer facilities, mobile training units, and community digital centres may therefore provide more inclusive alternatives.

4.3. Dimensional Interpretation of the Framework

The 11 survey indicators were grouped into three analytical dimensions: security-conscious agency, socioeconomic and access barriers, and empowerment and agency. **Table 4** summarizes these dimensions. Security-conscious agency produced the lowest aggregate mean, indicating the strongest agreement under the survey coding. This finding supports the conceptual proposition in **Figure 1** that cybersecurity awareness is a central requirement for safe AI participation. The socioeconomic-barrier dimension produced an average mean of 1.72. Device access, mobile data costs, and the absence of specialized AI-safety training affected participants' ability to engage consistently with AI tools. These are not solely individual problems. They require community and institutional responses, including shared digital infrastructure, locally accessible training, affordable connectivity, and partnerships among schools, colleges, local government, and nongovernmental organizations.

The empowerment-and-agency dimension also produced an average mean of 1.72. Participants recognized the academic and economic potential of AI, although perceptions of social empowerment differed across the sample. This combination indicates that rural girls

were interested in AI-related opportunities but required protective knowledge and enabling community conditions before those aspirations could be translated into sustained participation.

Table 4. Dimensional analysis of the community-based AI-empowerment framework.

DIMENSION	INCLUDED INDICATORS	AVERAGE MEAN	INTERPRETATION
Security-conscious agency	Q1, Q2, Q3, Q4	1.36	Critical priority
Socioeconomic and access barriers	Q5, Q6, Q7	1.72	Significant barrier and service need
Empowerment and agency	Q8, Q9, Q10, Q11	1.72	Strong but uneven aspiration

As shown by the interaction among the components in **Figure 1**, access, safety, and empowerment should be addressed together. Infrastructure without literacy may increase unsafe exposure, while safety education without practical access may remain theoretical. Similarly, empowerment messages without mentoring and community support may create expectations that cannot be sustained.

4.4. Regression Results for AI Empowerment

A multiple linear regression analysis was conducted to examine item-level associations between seven selected indicators and the AI-empowerment outcome. The model was statistically significant, $F(7, 998) = 20.95$, $p < 0.001$, and explained 12.8% of the variance in empowerment ($R^2 = 0.128$). The findings therefore indicate that the selected indicators were collectively associated with empowerment, although most of the variance remained unexplained by the model. As shown in **Table 5**, financial fraud and online scams were significantly associated with empowerment ($B = -0.082$, $p = 0.001$). The negative coefficient indicates that stronger perceptions of fraud-related barriers corresponded with lower empowerment scores, assuming that higher outcome scores represented stronger empowerment. This result highlights the importance of incorporating fraud awareness, account protection, scam identification, and reporting procedures into community-based AI-literacy programs.

Table 5. Multiple regression analysis of indicators associated with AI empowerment.

PREDICTOR	B	SE	*t*	*p*
Constant	1.803	0.152	11.832	<.001
Recognition of digital-safety risks, including image misuse and online traps	-0.043	0.034	-1.261	0.208
Financial fraud and online scams as barriers to independent use	-0.082	0.025	-3.300	0.001
Critical evaluation of inaccurate AI-generated information	-0.125	0.032	-3.955	<0.001
Prioritization of data privacy and responsible AI use	0.112	0.035	3.242	0.002
Mobile data cost as a financial burden	0.244	0.041	5.951	<0.001
Reliable access to a personal smartphone or computer	0.019	0.021	0.943	0.346
Perceived need for specialized AI-safety training	-0.067	0.045	-1.491	0.136

Note for model statistics: $F(7, 998) = 20.95$, $p < 0.001$; $R^2 = 0.128$.

Concern about inaccurate AI-generated information was also significantly associated with empowerment ($B = -0.125$, $p < 0.001$). This finding suggests that uncertainty about information accuracy may discourage independent AI use. Rural girls may recognize the

educational potential of AI while remaining hesitant because they lack confidence in verifying its outputs. Community-service activities should therefore include source checking, comparison with trusted references, recognition of AI hallucinations, and responsible academic use. Prioritization of data privacy and responsible AI use produced a significant positive coefficient (B = 0.112, p = 0.002). This result indicates that ethical and privacy awareness may support empowerment by enabling participants to use digital technology more confidently and responsibly. Protective literacy should consequently be treated as an integral part of AI education rather than as a separate technical topic.

Mobile data cost as a financial burden produced the largest coefficient (B = 0.244, p < 0.001). Because the item was phrased as a burden, this coefficient should not be interpreted as evidence that expensive mobile data improves empowerment. Rather, it demonstrates a statistically significant association whose direction depends on the coding of the item and the outcome variable. The result may indicate that participants with greater AI engagement were more aware of data expenditure, or that reverse coding affected the coefficient. Therefore, the result confirms the relevance of mobile data costs but does not establish them as a positive driver of empowerment.

Reliable device access was not statistically significant (B = 0.019, p = 0.346). This result does not imply that devices are unimportant. Device access may function as a basic enabling condition whose effect depends on connectivity, training, confidence, and community support. Similarly, the perceived need for specialized AI-safety training was not statistically significant (B = -0.067, p = 0.136), although its descriptive mean showed that participants considered such training important.

Recognition of general digital-safety risks was also not statistically significant (B = -0.043, p = 0.208). General awareness alone may therefore be insufficient to support empowerment. Participants may require practical skills that allow them to respond to risks, rather than simply recognizing that those risks exist.

The regression findings indicate that cybersecurity concerns, misinformation, privacy awareness, and connectivity costs were associated with AI empowerment. However, the analysis demonstrates association rather than causation and does not statistically establish security-conscious agency as a mediator. Accordingly, mediation remains a conceptual proposition of the framework. Future research should validate the proposed relationships using multi-item constructs, mediation analysis, or structural equation modelling.

The survey findings indicate that security-conscious agency was a critical component of AI participation among the predominantly rural female sample. Socioeconomic barriers and empowerment aspirations were also prominent, suggesting that access, safety, and motivation should be addressed together. Community-service programs should therefore combine affordable digital access, AI-skills training, misinformation awareness, privacy education, and sustained mentoring.

The results do not support the interpretation that access alone automatically produces empowerment. Instead, participants appear to require a supportive community environment in which families, peers, educators, and local institutions help them understand both the opportunities and risks associated with AI. This interpretation strengthens the community-based orientation of the framework and provides a practical basis for designing safe and inclusive AI-literacy interventions.

4.5. Community-Based Interpretation of Security-Conscious Agency

The findings support the conceptual importance of security-conscious agency for sustainable AI empowerment among rural girls, although its mediating role was not statistically tested in this study. Participants evaluated AI not only in terms of usefulness and access but also in relation to information accuracy, privacy, fraud, and potential misuse. They also considered whether AI-generated information was accurate, whether personal data were protected, and whether online engagement exposed them to fraud or misuse. This finding supports the central proposition of the framework that access and skills must be filtered through risk awareness before they can produce meaningful empowerment. The strong concern regarding inaccurate AI information is particularly important for community-service programs. Rural girls may use AI for academic work, information searching, communication, and future employment preparation, but these benefits can be weakened when users cannot distinguish reliable outputs from misleading or fabricated content. Community-based AI education should therefore include practical verification activities rather than only technical demonstrations. Participants should learn how to compare AI-generated information with textbooks, institutional sources, subject experts, and other trusted references.

The significant relationship between privacy awareness and empowerment also shows that protective knowledge can strengthen confidence. Participants who understand responsible AI use may be better prepared to make informed choices regarding personal information, images, account credentials, and digital communication. Community-service programs should therefore integrate privacy and ethical use across all AI-learning activities rather than presenting cybersecurity as a separate topic.

This interpretation is consistent with human-centered AI, which emphasizes reliable, safe, and trustworthy technological environments (Shneiderman, 2020). However, the present findings extend that perspective by showing that user-level protective agency is also necessary. Safe system design alone cannot guarantee safe participation when users lack critical digital literacy.

4.6. Socioeconomic Barriers and the Need for Community Infrastructure

Socioeconomic barriers continued to shape AI participation. Mobile data costs, uneven device access, and limited specialized training were associated with participants' ability to engage consistently with AI tools. These barriers should not be treated as individual weaknesses because they reflect broader infrastructural and economic conditions. The regression analysis confirmed that mobile data cost was significantly associated with empowerment. However, because the item was framed as a financial burden, the coefficient should be interpreted carefully. The finding demonstrates that connectivity costs matter, but it does not prove that higher costs improve empowerment. Rather, participants who used AI more frequently may have become more aware of data expenses, or the item may have required reverse coding before interpretation. From a community-service perspective, this result highlights the importance of shared digital infrastructure. Community centers, schools, colleges, and local training institutions can provide supervised internet access, shared devices, and structured AI-learning sessions. These arrangements may reduce the financial burden on individual participants and create safer environments for guided practice.

Community-based infrastructure can also address differences in device ownership. The descriptive results showed substantial variation in reliable access to smartphones or computers. Training programs that assume every participant owns a suitable device may

unintentionally exclude the most disadvantaged group. Shared laboratories, mobile learning units, scheduled computer access, and institution-supported connectivity are therefore more inclusive options.

Sociotechnical Systems Theory explains that technology outcomes depend on the alignment of technical infrastructure and social arrangements (Baxter and Sommerville, 2011). The present findings support this view. AI empowerment requires more than devices or software. It depends on affordable access, supportive institutions, relevant training, and trusted social environments.

4.7. Community Support as a Practical Service Mechanism

Within the proposed framework, community support functions not only as a contextual factor but also as a practical delivery pathway for AI-literacy and cybersecurity interventions. Families, teachers, peers, educational institutions, women entrepreneurs, local authorities, and nongovernmental organizations can contribute different forms of support.

Families play an important role because rural girls' technology use may be influenced by parental trust, social expectations, and concerns about online safety. Community-service programs should therefore involve family members rather than focusing only on students. Family information sessions can explain the educational benefits of AI while also addressing privacy, fraud, image misuse, and responsible use. This approach may reduce fear-based restrictions and replace them with informed supervision.

Teachers and educational institutions can provide structured learning and trusted guidance. AI workshops delivered through schools and colleges can connect digital tools with academic needs, such as information searching, language support, study planning, and content evaluation. Educators can also help students recognize inaccurate outputs and avoid overreliance on AI-generated material.

Peer networks can support continued participation after formal training. Participants may feel more confident when they can discuss problems with other learners, share experiences, and seek help. Peer mentoring is especially useful in rural settings where specialist trainers may not be continuously available. Trained participants can act as local digital ambassadors who support others in their communities.

Local organizations and women entrepreneurs can strengthen the practical relevance of AI training by connecting digital literacy with employment, small business, communication, and community leadership. Community-service programs should therefore combine educational, social, and economic objectives.

4.8. Community-Service Model for Rural Girls' AI Empowerment

The proposed service model was formulated by combining the quantitative findings with contextual issues identified during stakeholder consultations. It should therefore be interpreted as a practice-oriented framework rather than as an experimentally tested intervention. **Table 6** presents the seven interconnected stages of the proposed community-service model. Community service should be continuous rather than limited to a single workshop. Initial training may improve awareness, but participants also need opportunities to practice, ask questions, receive feedback, and update their knowledge as AI technologies change. The model also emphasizes that cybersecurity should be introduced before and

during AI use. Participants should not be encouraged to explore AI applications independently without understanding misinformation, privacy, fraud, and ethical risks. Protective literacy must operate as a cross-cutting component of every service stage.

Table 6. Proposed community-service model for AI empowerment among rural girls.

STAGE	MAIN ACTIVITY	RESPONSIBLE COMMUNITY ACTORS	EXPECTED OUTPUT
Community assessment	Identify device access, connectivity, safety concerns, training needs, and family attitudes	Schools, colleges, local authorities, community organizations	Local needs profile and participant mapping
Protective digital literacy	Teach fraud recognition, privacy protection, password safety, image protection, and misinformation verification	Educators, ICT volunteers, cybersecurity trainers	Improved security-conscious agency
Guided AI engagement	Provide supervised practice in educational AI use, information evaluation, responsible prompting, and academic integrity	Teachers, university volunteers, peer mentors	Safer and more meaningful AI use
Family and community engagement	Conduct family sessions, awareness campaigns, and local discussion forums	Families, community leaders, women's groups	Increased trust and social support
Access support	Provide shared devices, community internet access, and affordable training facilities	Institutions, local government, NGOs	Reduced infrastructural exclusion
Mentoring and follow-up	Establish peer groups, refresher training, and referral systems for digital problems	Peer mentors, schools, community centers	Continued participation and sustained empowerment
Evaluation	Measure changes in confidence, safety knowledge, AI use, and educational outcomes	Researchers, educators, community partners	Evidence for program improvement

4.9. Sustainable Community Development Implications

The proposed framework has broader implications for sustainable community development, particularly for the design of community-based digital literacy, cybersecurity education, and inclusive AI-support programs. AI empowerment can support education, information access, communication, employment preparation, entrepreneurship, and social participation. However, these outcomes are sustainable only when participants can use technology safely and independently. Community-based AI education can contribute to human-capacity development by strengthening digital confidence and critical thinking. It can also reduce gender-based exclusion by creating locally accessible learning opportunities for rural girls. When families and institutions are involved, the benefits may extend beyond individual participants to the wider community. The framework also supports local ownership. Rural girls should not be treated as passive recipients of technology. Their concerns, experiences, and aspirations should shape program design. Participatory planning can help ensure that training addresses relevant problems, including language barriers, academic needs, employment goals, and local safety concerns. Sustainability also requires

institutional continuity. Short-term externally funded projects may have limited impact if community members cannot maintain access, update training, or support new participants. Educational institutions and local organizations should therefore integrate AI literacy and cybersecurity into regular outreach, community engagement, and student-support programs.

4.10. Comparison with Existing Technology-Adoption Models

The Community-Based AI Empowerment Framework differs from conventional technology-adoption models in several ways. The Technology Acceptance Model emphasizes perceived usefulness and perceived ease of use as determinants of adoption (Davis, 1989). UTAUT extends this explanation through performance expectancy, effort expectancy, social influence, and facilitating conditions (Venkatesh *et al.*, 2003). These models help explain whether individuals are likely to use technology, but they do not fully explain whether participation is safe, independent, and sustainable. Rural girls may perceive AI as useful while still facing misinformation, fraud, privacy concerns, and social restrictions. The present framework therefore shifts the analytical focus from adoption to empowerment. Empowerment includes the ability to evaluate information, protect personal data, make independent decisions, and use technology to achieve educational and economic goals. Security-conscious agency is central because access without protective capability may increase vulnerability. The framework also gives community service a more active role. Social influence in UTAUT is generally treated as a predictor of use, whereas the present study conceptualizes community support as an organized intervention involving training, mentoring, family engagement, infrastructure, and institutional partnership.

4.11. Theoretical Contribution of the Framework

The framework integrates four theoretical perspectives. Sociotechnical Systems Theory explains the interaction between infrastructure, institutions, users, and community conditions (Baxter and Sommerville, 2011). Human-Centered AI provides the safety and trust orientation required for inclusive technology use (Shneiderman, 2020). The Capability Approach explains empowerment as the ability to convert available resources into valued outcomes. Social Capital Theory highlights the role of relationships, trust, and community networks. The principal theoretical contribution lies in proposing security-conscious agency as a conceptual link between enabling conditions and empowerment outcomes. Digital access, AI engagement, skills, and community support may not produce sustainable empowerment unless participants can recognize risks, evaluate information, protect themselves, and make informed decisions. However, the present regression analysis did not statistically test mediation. Therefore, security-conscious agency should be described as a theoretically proposed mediating mechanism rather than an empirically confirmed mediator. Future studies should employ validated multi-item scales and structural equation modelling to test the proposed pathways.

4.12. Practical Recommendations for Community Service

The results support several practical recommendations.

(i) Community-service programs should integrate AI literacy and cybersecurity rather than treating them as separate topics. Every AI-training activity should include verification, privacy, fraud prevention, and responsible-use components.

(ii) Family and community engagement should be included in program design. Rural girls may experience stronger support when parents, teachers, and community leaders understand both the opportunities and risks of AI.

(iii) Training should be practical and scenario-based. Participants should practice identifying misleading outputs, protecting accounts, evaluating sources, and responding to suspicious messages.

(iv) Shared infrastructure should be developed for participants who lack reliable devices or affordable internet access. Schools, colleges, libraries, and community centers can serve as local digital-learning hubs.

(v) Community-service activities should include follow-up support. Peer mentoring, refresher sessions, local help desks, and educator networks can strengthen continuity.

(vi) Program evaluation should measure not only the frequency of AI use but also safety knowledge, confidence, critical evaluation, responsible behaviour, and educational benefit.

4.13. Study Limitations and Future Research

The findings should be interpreted in light of several limitations. The study was conducted in one district in Bangladesh, which limits generalizability to other rural regions. The quantitative sample was recruited through convenience sampling, and the dataset was predominantly female and rural, reducing the strength of formal group comparisons. The study also relied on self-reported responses. Because stakeholder consultations were used only to support contextual interpretation, the study did not present a full independent qualitative analysis or direct participant quotations. Participants may have overestimated or underestimated their AI knowledge, safety awareness, or empowerment. Group-administered surveys may have created social-desirability effects despite efforts to protect anonymity. The framework was examined using item-level regression rather than validated latent constructs. Therefore, the analysis did not test the complete theoretical model or confirm the proposed mediating mechanism. The modest value of R^2 also indicates that other influences on empowerment were not included. Future studies should validate the framework across multiple districts using probability sampling. Longitudinal research should examine whether community-service interventions produce sustained changes in AI use, cybersecurity behaviour, educational participation, and economic opportunity. Structural equation modelling may also be used to test the relationships among access, community support, security-conscious agency, and empowerment. Further research should include rural girls with disabilities and participants from different age, educational, linguistic, and socioeconomic groups. Comparative studies involving rural and urban communities may clarify how infrastructural and social conditions influence AI empowerment.

5. CONCLUSION

This study developed a community-based Artificial Intelligence (AI) empowerment framework for rural girls in Bangladesh by integrating digital literacy, cybersecurity, community support, and sustainable community development. The findings indicate that AI empowerment depends not only on digital access but also on security-conscious agency, including the ability to evaluate information, protect personal data, and recognize online risks. Community service provides a practical mechanism for translating these dimensions into educational interventions through collaboration among schools, families, local institutions, and community organizations. Future studies should validate the proposed

framework using larger samples, multiple regions, and structural equation modelling to strengthen its generalizability and theoretical robustness.

6. ACKNOWLEDGMENTS

This study sincerely acknowledges all students, educators, researchers, women entrepreneurs, interview participants, and focus group members who contributed their time and perspectives. Appreciation is also extended to Nizam Uddin Ahmed Model College and the participating community institutions in Sherpur Sadar Upazila for supporting the research process.

7. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. The authors confirmed that the paper was free of plagiarism.

8. REFERENCES

Abosede, P. J., Idris, I. A., Adeola, I. M., Glory, T., and Stephen, G. O. (2025). Community service assessment of demographic predictors of undergraduates' readiness to use artificial intelligence (AI) tools for learning. *ASEAN Journal of Community Service and Education*, *4*(2), 77-90.

Amado, J. A., and Digo, G. S. (2026). Developing an artificial intelligence (AI)-guided financial management toolkit: The role of school heads' leadership styles and practices. *ASEAN Journal of Economic and Economic Education, 5*(1), 35-48.

Baxter, G., and Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4-17.

Bolaji, H. O., Ahmed, A. T., Ibrahim, A., Jimba-Na'Allah, F. K., Oyeyemi, W. T., Hassan-Ibrahim, R. B., and Luwoye, A. (2025). Gender as a predictor of students' performance in physics education technology simulation of chemistry content as community service in secondary schools. *ASEAN Journal of Community Service and Education*, *4*(2), 123-132.

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Davidson, V. C., Maduegbunam, T. O., Odo, J. A., Adony, I. I., Ugwuarua, F. S., and Agbo, C. N. (2026). Integrating artificial intelligence (AI) in mathematics education: Enhancing students' interest and achievement through adaptive learning systems. *ASEAN Journal for Science Education, 5*(1), 87-94.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Jimoh, A. B., Makind, S. O., and Abdullahi, A. (2027). The risks associated with drug abuse and addiction on the academic performance of Niger State College of Education students in the artificial intelligence era: Implications for community service and education. *ASEAN Journal of Community Service and Education, 6*(1), 23-30.

Karmaker, R. (2025a). Educational impact and trends of ethnic language loss in Bangladesh: A statistical and policy-based review (2013-2023). *ASEAN Journal of Educational Research and Technology*, *4*(3), 295-310.

Karmaker, R. (2025b). Community service as a strategy for indigenous language revitalization in Bangladesh. *ASEAN Journal of Community Service and Education*, *4*(1), 1-8.

Karmaker, R. (2026). Economic marginalization and indigenous ethnic language loss in Bangladesh. *ASEAN Journal of Economic and Economic Education*, *5*(1), 1-6.

Karmaker, R., and Cvetković, V. M. (2025). Digital literacy and educational empowerment among rural women in Bangladesh: Bridging the technology access gap. *International Journal of Disaster Risk Management, 7*(2), 239-262.

Katel, K. (2026). Artificial intelligence (AI) ChatGPT in academic and science writing education: Student dependency, creativity, and the mediating role of feedback in English as a second language and English as a foreign language contexts. *ASEAN Journal for Science Education, 5*(2), 155-166.

Nagaraju, K., and Ramakrishna, S. (2025). Leveraging artificial intelligence (AI) and geospatial technologies for community-centered urban expansion forecasting in Hyderabad. *ASEAN Journal of Community Service and Education*, *3*(2), 135-146.

Nnanguma, K. A. (2025). Integrating artificial intelligence for climate-smart agriculture and sustainable food systems. *ASEAN Journal of Agriculture and Food Engineering*, *4*(2), 71-80.

Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe, and trustworthy. *International Journal of Human-Computer Interaction, 36*(6), 495-504.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.