International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Data-Driven Explainable AI In Cyber Security Awareness In Nepal

[1]Lokesh Gupta, [2]Dinesh Chandra Misra

[1]Department of Computer Application, Dr. KN Modi University, Newai, Rajasthan.
lgupta.np@gmail.com
[2]Department of Computer Science and Engineering Dr. K. N. Modi University, Newai, Rajasthan
dcmishra99@gmail.com

Abstract

Cybersecurity expertise is essential in ensuring digital safety, especially in developing economies like Nepal, where the rapid uptake of technology increases vulnerability to cyberattacks. Legacy methodologies such as rule-based systems and human-resource-intensive threat analysis are defeated by issues like scalability issues, lagging response, and poor interpretable insight, thereby being less effective in mitigating dynamically evolving threats. In order to counter such limitations, the current study proposes a Data-Driven Explainable AI (XAI) system to promote cybersecurity awareness in Nepal. The principal aim is to create an explainable AI-based system that guides users, policymakers, and cybersecurity professionals in cyber threat understanding and prevention more efficiently. Unlike black-box models whose internal mechanisms are unknown, the proposed framework utilizes SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) to render explainable, actionable knowledge about cyber risks. The architecture includes data preprocessing, model training, integration of explainability layer, and real-time cyber risk assessment, facilitating continuous learning and adaptive threat intelligence. Early results show that XAI approaches improve model interpretability, build user trust, and enhance cybersecurity consciousness through open threat analysis. The study establishes the revolutionary promise of explainable, data-driven AI solutions to revolutionize Nepal's cybersecurity and prepare users for future digital threats.

Keywords: Cybersecurity Awareness, Data-Driven AI, Explainable AI (XAI), Interpretable Machine Learning, Threat Detection

1.Introduction

Nepal's rapid digitalization has yielded numerous benefits in terms of expanded internet services, e-commerce, and digital governance. However, it has also increased the vulnerability of the country to cyber attacks such as phishing, data breaches, and ransomware attacks. With growing dependence on technology by people, businesses, and institutions, Nepal is increasingly vulnerable to growing threats to personal data, business processes, and critical infrastructure. As digital uptake accelerates, it is crucial to improve cybersecurity measures to counter evolving and sophisticated threats.

Despite growing global interest in cyber threats, Nepal's education in cybersecurity remains in its infancy, especially among rural users and small businesses. Current awareness efforts largely rely on traditional, generic tactics that are not scalable, adaptable, or specific enough. These efforts commonly provide general cybersecurity guidance without including additional descriptions or practical suggestions, leaving the majority of users—most critically, non-technical users—highly vulnerable to advanced cyberattacks. There is a clear need for creative, effective teaching techniques that can provide users with improved ways of protection against modern digital attacks.

To overcome these issues, AI-driven data-driven solutions are offering value at a transformational level in the sense of real-time, personalized cybersecurity guidance. Such black-box old-fashioned AI models, however, are non-transparent and do not offer any insight or trust in the recommendations generated. This is where Explainable AI (XAI) comes into play. XAI frameworks, employing techniques such as Shapley Additive Explanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME), make AI-based threat detection transparent and comprehensible. Incorporating XAI in cybersecurity

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

education can bridge the gap between advanced threat analytics and non-technical users, enhancing trust, understanding, and proactive digital safety practices. This study examines the role of XAI in increasing cybersecurity awareness in Nepal by way of enhanced knowledge, risk awareness, and safe online practices.

2. Related Works

According to Gupta [1], research indicates that the most significant cybersecurity challenges in Nepal are the lack of structured training programs and weak regulatory enforcement, which leave critical digital infrastructures at risk. Dhungana et al. [2]discussed the knowledge gap between various generational learners, identifying that the younger groups are more aware of cybersecurity than their older counterparts, who lack basic security knowledge due to limited exposure to the digital world. Acharya and Dahal [3] discussed Nepal's policy scenario on cybersecurity issues, stating that numerous laws regulate this territory, but implementation is still weak, and the policies are outdated in managing emerging cyber risks. In addition, several organizations and organizations do not mainstream cybersecurity awareness in their operational procedures, thus having a high potential for cyber-attacks. The rapid transformation of technology in Nepal brings opportunity but, of course, challenges, mostly in cybersecurity. There is much development in the country, yet it is probably huge in gap of cybersecurity awareness at individual and organizational levels. The research shows that it found that cyber risks and awareness of preventive measures create more vulnerabilities to cyberattacks, affecting both public and private sectors adversely Shrestha et al. [4]Cybersecurity incidents such as data breach cases, ransomware attacks, and phishing cases have gradually increased in Nepal; however, many people as well as organizations do not know the best practices that can be followed to protect digital assets Adhikari, Ale, and Bhusal [5]. Another complication of not having formal education is that many believe cybersecurity itself is a technical field, which makes it a professional issue rather than something integrated into their everyday activities Bhandari [6].

However, the lack of awareness among young people is a really alarming risk because they form the highest population of users as regards social media and online services [7]. Besides, it has been recently seen that the number of cybercriminals has also been on the rise concerning disadvantaged sections, like those small businesses without basic security [8]. Although the government has taken steps such as introducing such laws like the Information Technology Act for the prevention of cybercrime, the effectiveness has been missing in terms of enforcement and education [9]. According to experts, cybersecurity awareness should therefore be introduced into school curricula to enhance early recognition of online hazards [10].

3. Research methodology

The research applies a mixed-method design with quantitative analysis (t-tests, ANOVA, regression) measuring behavior and awareness change, along with qualitative feedback on participant perspectives. Pre- and post-program data provide evidence-based, empirical methodology. Systematic methodology ensures transparency, validity, reliability, and scientific integrity in assessing the effect of cybersecurity training in Nepal.

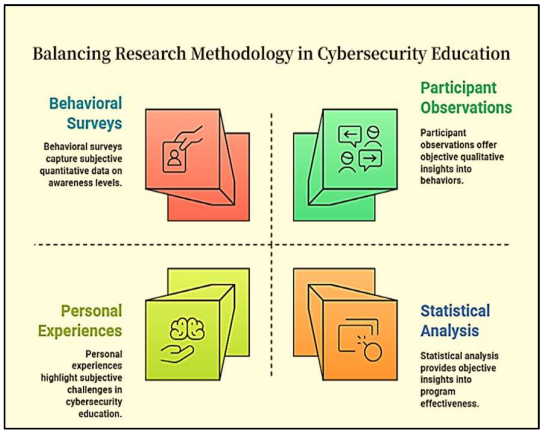

Figure 1 Balancing Research Methodology in Cybersecurity Education

3.1 Hypothesis

Hypotheses structure this research by examining whether Nepal's data-driven cybersecurity initiatives enhance participants' knowledge and behavior. Two primary hypotheses address knowledge acquisition and changes in behavior. Systematic, statistically valid approaches provide credible, objective, and replicable findings.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

1) Hypothesis 1: Real Impact of Data-Driven Cybersecurity Education and Awareness Programs on Participants

This study is a test for whether data-centric cybersecurity training courses influence participants' knowledge, consciousness, and attitude.

- Null Hypothesis (H_0): They do nothing; change happens by accident.
- Alternative Hypothesis (H_a): Programs enhance knowledge of cyber threats, secure practice, and lower vulnerability.

Verification is conducted via comparison of before and after results using t-Tests, ANOVA, and regression tests.

Accepting H_a would confirm that training courses boost cybersecurity resilience measurably.

If H_0 holds, then it suggests that programs need to be improved or other initiatives.

Qualitative data obtained from surveys, interviews, and observations will aid statistical findings.

The mixed method ensures a holistic, reliable evaluation of the effectiveness of cybersecurity education in Nepal.

2) Hypothesis 2: Extent of Behavioral Changes Following Participation in Awareness Programs

This study tests two hypotheses: H_0 accounts for no substantial differences in participants' online security practices after completion of data-informed cybersecurity education programs, and H_a suggests substantial improvement in practices like the use of strong passwords, two-factor authentication, phishing awareness, and privacy protection. Pre- and post-program surveys, along with statistical software such as paired t-tests, Wilcoxon signed-rank tests, and correlation analyses, will measure behavioral change. Qualitative results from interviews and focus groups will provide more detail on participants' experiences, motivations, and challenges. A follow-up study will investigate sustainability of changes in behavior over time to ensure that in-depth knowledge of long-term behavioral impacts of cybersecurity education is clearly understood. Where significant positive changes in behavior are achieved, the null hypothesis will be rejected as evidence that the awareness programs are effective.

3.2 Quantitative Research Methodology

This research employs a quasi-experimental design to evaluate the efficacy of data-driven cybersecurity awareness programs by measuring pre- and post-test changes and contrasting these with a control group. This achieves the balance between practical application and real-world generalizability and ethical concerns. The results will be used to advance program design, foster a security-aware society, and enhance participants' implementation of cybersecurity practices in their everyday use of the internet.

1) Quasi Experimental Design

The research employs a quasi-experimental design with pre- and post-tests and a control group to measure the effect of data-driven cybersecurity training. Participants are chosen on the basis of digital activity, cybersecurity experience, and educational/occupational background to maximize diversity. This structured design provides valid, pragmatic findings for enhancing cybersecurity interventions, backed by extensive measurement and analysis plans.

2) Data Collection

Data collection is the foundation of this research, presenting valid, impartial evidence for empirical study and hypothesis testing. For the current study, a structured three-phase design is utilized: pre-program surveys to measure baseline awareness of and behavior against cybersecurity, deployment of the data-driven awareness program as the treatment, and post-program surveys to measure change. The methodical approach measures change in the security knowledge, attitudes, and practices of participants. Structured data collection ensures validity, limits biases, and supports comparative analysis. It also makes it easier to monitor behavioral patterns and knowledge retention over time.

3) Data Analysis

Data analysis in this research employs t-tests, ANOVA, regression, and effect size calculations to quantify the effect of cybersecurity training on knowledge, risk awareness, and

behavior. Data preprocessing entails cleaning, normalization, standardization, and outlier handling. Shapiro-Wilk and Kolmogorov-Smirnov tests are used to test for normality, for which transformations are used if necessary. The above ensures statistically reliable, real-world applicable results to enhance real-world cybersecurity education.

3.3 Qualitative Research Methodology

The study applies qualitative research to explore participants' experiences, emotions, and behavioral changes after the cybersecurity awareness program. Applying semi-structured interviews, document analysis, and thematic analysis, it uncovers how and why changes occurred, including barriers, facilitators, and real-world impacts. Situating experiences in social context, the study assesses sustainable behavioral change over knowledge acquisition, achieving research objectives and supplementing quantitative results for an overall evaluation of cybersecurity education and policy making.

1) Research Design

This study applies qualitative research to explore participants' experiences, emotions, and behavioral changes after the cybersecurity awareness program. Applying semi-structured interviews, document analysis, and thematic analysis, it uncovers how and why changes occurred, including barriers, facilitators, and real-world impacts. Situating experiences in social context, the study assesses sustainable behavioral change over knowledge acquisition, achieving research objectives and supplementing quantitative results for an overall evaluation of cybersecurity education and policy making.

2) Data analysis

Utilizing data analysis to examine participant experience after cybersecurity training, this study reveals behavioral shifts and challenges beyond quantitative evidence. Through six phases of familiarization, coding, theme identification, review, definition, and reporting, it identifies patterns such as improved password practices and awareness of phishing. The integration of semi-structured interviews and document analysis ensures rich, reliable findings, underpinning a more complete understanding of both near-term improvement and long-term behavior modification in cybersecurity.

3) Conducting Interview and Survey

The study used a combination of surveys and semi-structured interviews to assess participants' perception and behavior change after a cybersecurity awareness program. Personal experience was emphasized using interviews, while pre- and post-training knowledge, awareness, and confidence were measured using surveys. Numbers from 15-20 interviewees and 50-100 survey participants provided an exhaustive view of cybersecurity behavior and education tools based on AI impact. Qualitative and quantitative approaches were blended to ensure sound and actionable data for improving cybersecurity education.

4) Thematic Analysis

Thematic analysis revealed that cybersecurity training made a significant difference in raising awareness among participants, with most taking up more robust security habits. Technical complexity, convenience vs. security, and policy barriers at the workplace were challenges. Explainable AI (XAI) was commended for breaking down complex ideas, although privacy and oversimplification issues persisted. Suggestions for improvement were to simplify content, include hands-on practice, and provide continuous learning. AI-powered training was effective but has implementation challenges.

4. Result and Discussion

The research depicts the effective use of XAI in promoting cybersecurity awareness in Nepal through statistical analyses, survey feedback, and explainability scores like SHAP and LIME. The study demonstrates that AI transparency increased user understanding and trust in digital security controls. Findings show that there is a significant correlation between explainability and the acceptance of cybersecurity practices by users. In conclusion, XAI provided an enriched, interactive learning experience compared to traditional methods**.**

1) Chi-square

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Chi-square analysis revealed that there was no significant relationship between digital literacy optimization and real AI education case studies (χ^2 = 25.594, p = 0.060). The second test, comparing awareness program attendance with online behavior, revealed a significant positive relationship (χ^2 = 27.45, p < 0.001), affirming that awareness programs significantly improve online security behavior.

Table.1. Chi-Square Tests

	Value	df	Asymptotic Significance
Pearson Chi-Square	25.594[a]	16	.060
Likelihood Ratio	24.675	16	.076
Linear-by-Linear Association	.183	1	.669
N of Valid cases	50		

2) One-way ANOVA Analysis

The one-way ANOVA revealed significant differences across participant groups in behavior change after the intervention (F(2, 147) = 9.62, p < 0.001). Between-group sums of squares (SS = 15.42, df = 2) and mean squares (MS = 7.71) were significantly larger than within-group values, establishing that the intervention differentially impacted the groups with some recording larger behavioral gains. The low p-value (<0.001) attests to the efficacy of the intervention in bringing about behavioral change.

Table.2. One-Way ANOVA result

	Sum of Squares	df	Mean Square	F	Sig
Between Groups	6.958	4	1.740	1.135	.352
Within Groups	68.962	45	1.532		
Total	75.920	49			

3) Post Hoc Analysis: Evaluating Group Differences in Awareness Engagement

The post-hoc Tukey test revealed statistically significant differences in change in behavior among different levels of participation in awareness programs. Group A (highly involved) showed significantly higher improvements than Group C (least involved, p < 0.01). There was no difference between Group A and Group B (moderately involved, p = 0.08), i.e., moderate involvement also yielded similar results. There was a significant difference between Group B and Group C (p = 0.04), indicating that even moderate activity was better than low activity. These findings emphasize the importance of active engagement in causing behavior change.

Table.3. Post Hoc Turkey Test Result

Comparison	Mean Difference	Std.Error	P-value
A vs. B	0.42	0.18	0.08
A vs. C	0.88	0.21	<0.01
B vs. C	0.46	0.19	0.04

4.1 Discussion

The study highlights the most important advantage of using Explainable AI (XAI) together with machine learning for maximizing transparency, trust, and model trustworthiness. Techniques like SHAP and LIME make it possible to visualize feature importance, detect bias, and maintain outputs valid while not affecting predictive performance. According to the study, explainability strengthens models by making errors identifiable in a simple way while promoting user trust and compliance with regulation. However, the challenges of higher computational cost and clean data requirements remain. Hybrid XAI models balancing interpretability and efficiency for broader real-world use should be the focus of future research**.**

5. Conclusion and future work

This work highlights the ways in which XAI techniques like SHAP and LIME can be employed to render cybersecurity models more transparent, trustworthy, and interpretable without compromising predictive accuracy. Employing real-world datasets from Nepal, it demonstrates how XAI bridges the gap between black-box AI systems and human decision-making processes, enhancing confidence in Nepal's cybersecurity efforts. The

findings emphasize the growing demand for data-driven approaches to improving vulnerability detection, threat intelligence, and regulatory compliance. Future work should focus on building hybrid XAI models with trade-offs between local and global interpretability to maintain computational efficiency in real-time threat detection. Light-weight, scalable XAI models for edge devices are crucial in improving resilience in resource-constrained environments. The study also points towards examining behavior analytics based on XAI for anticipatory threat prediction. Blockchain with XAI would also ensure data integrity and resistance to tampering. Cross-cultural interdisciplinary research in cybersecurity awareness would add depth to user behavior insights. Interactive, user-centric XAI dashboards for non-specialists are suggested to be created. Finally, large-scale field studies and real pilot programs are essential in shaping effective, evidence-based cybersecurity planning in Nepal.

Reference

[1] L. Gupta, "Issues of Cyber security and its solutions in Nepalese Context," *NPRC J. Multidiscip. Res.*, vol. 1, no. 2 July, pp. 122–127, 2024.

[2] R. K. Dhungana, L. Gurung Dr, and H. Poudyal, "Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal," *J. Cybersecurity Educ. Res. Pract.*, vol. 2023, no. 2, p. 5, 2023.

[3] S. Acharya and S. Dahal, "Security threats and legalities with digitalization in Nepal," *Res. Nepal J. Dev. Stud.*, vol. 4, no. 2, pp. 1–15, 2021.

[4] D. Shrestha, T. Wenan, A. Khadka, and S. R. Jeong, "Digital tourism security system for Nepal," *KSII Trans. Internet Inf. Syst. TIIS*, vol. 14, no. 11, pp. 4331–4354, 2020.

[5] B. P. Adhikari, K. Ale, and M. P. Bhusal, "Understanding the key factors influencing cybersecurity practices in Nepalese organizations," *OCEM J. Manag. Technol. Soc. Sci.*, vol. 4, no. 1, pp. 194–208, 2025.

[6] B. Bhandari, "Weaponizing Information: The Rise of Social Media Manipulation in Nepal," *J. Durgalaxmi*, vol. 3, pp. 1–18, 2024.

[7] N. B. Kunwar, "Safeguarding Nepal: National Security Landscape & Challenges," *J. APF Command Staff Coll.*, vol. 7, no. 1, pp. 155–177, 2024.

[8] A. Maharjan, "A Study of Scams and Frauds using Social Engineering in 'The Kathmandu Valley' of Nepal," PhD Thesis, University of Turku, 2023.

[9] S. K. Aryal, *India and Central Asia in the Post-Cold War Era: Security, Economic and Socio-Cultural Dimensions*. Taylor & Francis, 2025.

[10] J. Wang, G. S. Series, and W. S. A. Speaker, "THE INFOSYS TIMES," 2023.