International Journal of
Human Computations and Intelligence
Vol. 05, Issue. 02, 2026

RESEARCH ARTICLE OPEN ACCESS

Cybersecurity Awareness Level: An Analytical Assessment of Knowledge, Practices, and Attitudes

P Sumalatha* . D Sunil Kumar . M Santhosh . B Vandana . D Harshavardhan

Department of CSE (IoT, Cyber Security including Block Chain Technology), Annamacharya Institute of Technology & Sciences (Autonomous), Tirupati, A.P, India.

DOI: **10.5281/zenodo.18596159**
Received: 19 January 2026 / Revised: 29 January 2026 / Accepted: 10 February 2026
*Corresponding Author: *psumalatha241@gmail.com*

Abstract – Human factors are a significant factor in the security threat landscape, especially in the increasing trend of adopting digital technologies. This paper discusses a data-driven evaluation of security awareness, knowledge, practices, and response capacity of individuals in the central part of India. Our approach relies on a set of 284 valid responses from a survey that assessed four aspects: background knowledge, awareness of cybercrime, education level, and ability to cope with cybercrime. Reliability tests show that the instrument has acceptable internal consistency reliability, with a Cronbach's alpha value of 0.67. Our regression analysis shows that awareness of cybercrime has the highest impact on the ability to cope with cybercrime, followed by background knowledge and education level, all of which are statistically significant at $p < 0.05$. In addition, this paper also discusses a web-based Cyber Security Awareness Level Assessment System, which facilitates the automation of data collection, evaluation, and analysis in assessing the level of security awareness among individuals in a particular institution and geographical location. Our proposed system helps transform subjective security awareness into objective security metrics, which are crucial in developing an effective security training plan and security policy. Results emphasize that cognitive awareness and educational exposure are statistically dominant predictors of cyber readiness, supporting the development of adaptive training models and evidence-driven cybersecurity policies. The architecture is scalable, modular, and suitable for institutional deployment, longitudinal studies, and regional cyber risk profiling.

Index Terms – Cybersecurity Awareness, Human-Centered Security, Cybercrime, Statistical Analysis, Survey-Based Assessment, Awareness Modeling, Web-Based System.

I. INTRODUCTION

The fast pace of digitalization in contemporary organizations, enabled by various technologies like cloud computing, IoT, big data, and interconnected enterprise systems, has dramatically changed the

MILESTONE RESEARCH.IN OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

security environment in a significant manner. Although the benefits of digitalization include improved efficiency, flexibility, and innovation, the increased complexity of the digitalized environment makes the organization vulnerable to sophisticated cyberattacks, such as advanced persistent threats (APTs), zero-day exploits, ransomware, insider attacks, and AI-powered social engineering [1]. The conventional method of cybersecurity management, which is static, compliance, and reactive, is no longer sufficient to cope with new cyber threats. Hence, the need for intelligent, dynamic, and data-driven cybersecurity management practices, along with AI technologies, is increasingly being recognized [2].

Artificial Intelligence (AI) and Machine Learning (ML) technologies have revolutionized cybersecurity, moving from a rule-based defense mechanism to a predictive, autonomous cybersecurity ecosystem. AI-based systems can handle large volumes of security logs, network traffic data, and user behavior patterns to identify security breaches, predict potential security threats, and respond in real time [3]. From a policy and procedure development perspective, AI technologies play a significant role in cybersecurity, not only in defense mechanisms but also in strategic decision-making. For instance, generative AI technologies can predict potential security breaches, test the efficacy of existing security mechanisms, and suggest modifications to security policies according to identified vulnerabilities and risk patterns [4].

This helps organizations transition from periodic policy updates to dynamic policy evolution, ensuring that cybersecurity procedures are continually updated in line with the evolving security environment [5]. Another significant advantage of AI-driven cybersecurity governance is its automation and optimization. AI algorithms can automatically evaluate the compliance of processes with security policies, detect anomalies in the defined processes, and send notifications or recommendations for improvement. This reduces the chances of human error, and the process is optimized for efficiency. Moreover, AI facilitates risk-informed policy development, which combines threat intelligence, asset value, and vulnerability data to inform the application of security controls and resource allocation. This is particularly important in large-scale environments and critical infrastructure sectors, where manual monitoring and administration of policies are not feasible.

However, there are concerns about the governance of such an infrastructure in which AI is integrated into cybersecurity policy. For instance, there are concerns regarding the legal, ethical, and accountability aspects of such an autonomous decision-making system, especially where such activities are conducted on critical infrastructure and/or user data [6]. Scholars have argued for the need to develop an appropriate governance framework that addresses the balancing of AI with legal, ethical, and human oversight [7]. It is therefore imperative to ensure that such an AI-based cybersecurity process aligns with appropriate cybersecurity frameworks, such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and risk governance [8], [9]. While there have been significant developments in AI-based applications for threat detection and response, there are limited research studies that explore AI's potential in developing and refining cybersecurity policies and procedures. Most research studies, as found, have focused on technical performance metrics, while the organizational, procedural, and policy-oriented dimensions of AI’s potential for supporting cybersecurity management practices require further research. In order to fulfill this research gap, this present research aims to explore AI-based opportunities for developing adaptive cybersecurity policies, procedural changes, and strategic decisions through data analytics and intelligent modeling. By integrating recent developments and governance approaches, this

present research aims to offer a holistic view of AI-based opportunities for improving cybersecurity resilience, response time, compliance, and organizational preparedness against cyber threats [10].

Our contributions are as follows:

- We propose a multi-dimensional human-centric cybersecurity awareness model that measures Background Knowledge, Cybercrime Awareness, Education Level, and Response Capability, thus enabling the conversion of behavioral security variables into analytical variables.
- We design a web-based Cyber Security Awareness Level Assessment System that automates user management, survey processing, awareness scoring, and statistical analysis within a single, modular analytical framework.
- We present a data-driven scoring and prediction method that uses reliability analysis and multivariate regression to identify the key predictors of cyber readiness and response capability.
- We evaluate cybersecurity awareness as an analytical process that supports real-time analysis, data management, and decision-making for training and planning.

II. LITERATURE SURVEY

As digital technologies are rapidly growing, the concept of cybersecurity awareness has become one of the most important elements in preventing the occurrence of cyber risks, especially those that could be caused by the human factor and not the technical flaws. The most recent literature is becoming more and more human-focused, focusing on the role of awareness, knowledge, attitudes, and training in cybersecurity behavior at the individual, educational, and organizational levels. On the individual level, McGregor et al. [11] theorized personal cyberspace and developed the concept of the Personal Cyber Risk Profile Model, in which cybersecurity awareness is found not to be a direct predictor of cyber risk reduction. Rather, there is the mediating effect of cyber knowledge between awareness and risk reduction. The study is a valuable addition to the human-centered cybersecurity research by providing a clear picture of how the indirect mechanism of awareness works, but due to the self-reported and cross-sectional nature of data, it cannot be generalized.

On the behavioral facet, Gwenhure [12] used a modified Health Belief Model (HBM) to examine the security behavior of university students towards email phishing attacks. The results demonstrate that perceived severity, perceived importance, self-efficacy, and cues to action are important predictors of secure behavior, but perceived susceptibility and barriers are not. The book makes contributions to the literature by bringing a health-based psychological perspective to the study of cybersecurity, filling the gaps that have been left by most literature in the field, which has presented technical awareness research, albeit with constraints of convenience sampling and perceived, and not factual, behavior. In order to measure cybersecurity awareness systematically, a number of researchers have paid attention to scale development. The Academia Information Security Awareness Scale (AISS) developed by Rohan et al. [13] is a multidimensional scale that includes such aspects of knowledge, attitude, behavior, individual responsibility, and social influence in higher education institutions. In the same manner, Arpaci et al. [14] have created Cybersecurity Awareness Scale (CSAS) for social media users with a focus on confidentiality, trust, and privacy. Both studies present validated measurement instruments in the literature

that address critical gaps in user-centric assessment of cybersecurity, but their reliance on self-reported information and sample context limits external validity.

Using PLS-SEM to discuss the connections between cybersecurity awareness, attitude, intention, cyber judgment, and adoption, Adeshola and Oluwajana [15] investigated the relationships between these variables among university students. Their results show that awareness plays a significant role in influencing adoption via attitude and intention, but cyber judgment moderation plays an insignificant role. The article demonstrates the importance of cognitive decision-making in cybersecurity behavior, but its methodological drawbacks (i.e., cross-sectional design, convenience sampling) remain. In the case of technology-enhanced learning settings, Oroni et al. [16] hypothesized a composite model that associates e-learning engagement, cybersecurity awareness, and information security policy compliance with the outcomes of cyber safety. Through the use of PLS-SEM and fsQCA, the research illustrates that cybersecurity awareness and policy compliance have a direct positive relationship with cyber safety, and e-learning engagement has an indirect positive relationship with these relationships. The configurational approach is a methodological improvement of linear models, even though it is restricted in generalizability.

Taherdoost [17] acknowledged the weaknesses of conventional methods of awareness and proposed the Integrated Cybersecurity Awareness Training (iCAT) model that integrates micro-learning, gamification, serious games, and knowledge graphs. The model solves the challenges of low interaction and retention in the traditional training programs as it provides interactive and adaptive learning experiences. Although the model is promising, its validation needs to be conducted at a large scale in different organizational environments. With a trend in data-driven viewpoints, Abuabid [18] introduced a machine learning-assisted model of cybersecurity situational awareness, which examines the human and organizational aspects. The results find that the strongest predictor of situational awareness is social resources, and the need to focus on both the organizational and social aspects of cybersecurity that should not be overlooked in favor of individual knowledge. However, the research is constrained by both surveys and contextual limitations.

The awareness training has been critically tested at the organizational level. In order to determine the effectiveness of phishing training, Ho et al. [19] performed a large-scale randomized controlled experiment with more than 19,500 employees. They find that when phishing failure rates are measured by annual awareness training, there is little effect, and this finding contradicts common expectations regarding the effectiveness of training. To this effect, Hillman et al. [20] assessed phishing simulations at enterprise scale and showed that personalization and organizational context have a significant impact on the phishing rates of clicking, whereas training timing has less immediate impact. Both articles present uncommon large-scale, real-world proofs but are limited to one-organization contexts and phishing conditions.

Generally speaking, it can be concluded that the literature reviewed is characterized by a distinct change in the focus of the strictly technical cybersecurity solutions to the human-focused, behavioral, and data-driven solutions. Although there have been significant advancements in the explanation of awareness, behavior, and training effectiveness, there are still gaps in longitudinal validation, real-world measurement of behavior, and incorporation of adaptive training models. There is still a need to conduct more research in this field.

III. PROPOSED SYSTEM ARCHITECTURE

The presented system is a web-based, structured, and data-driven framework for measuring cybersecurity awareness among users in Central India, incorporating user participation, surveys, and statistical analysis to generate reliable outcomes in an easily interpretable manner. The conceptual architecture of the proposed system can be divided into six different components: the Web Interface, the User Module, the Admin Module, the Survey Engine, the Statistical Analysis Module, and the Structured Datasets. All the components play a vital role in the secure processing of the data.

1) Web Interface Layer: The primary layer of communication between users, administrators, and backend services is the web interface. Request routing, session processing, and authentication are all under its control. There are two established access paths:
   - **User access** for registration, login, survey participation, and outcome visualization.
   - **Administrator access** for user verification, dataset control, and analytical review.

   To ensure role-based isolation and system security, all incoming requests are forwarded to the appropriate modules according to access privileges.
2) User Module and Authentication Model:
   Let,

$$U = \{u_1, u_2, \dots \dots \dots u_n\}$$

   define the set of registered users. Every user u_i is connected to a profile vector:

$$D_i = [g_i, a_i, o_i, r_i]$$

   where, $g_i, a_i, o_i,$ and r_i describe gender, age, group, occupation, and region, respectively.
   Only after administrative verification is user involvement made possible. This activation process removes duplicate or invalid entries and ensures the data's legitimacy. Users can submit survey answers and get calculated awareness feedback after verification.

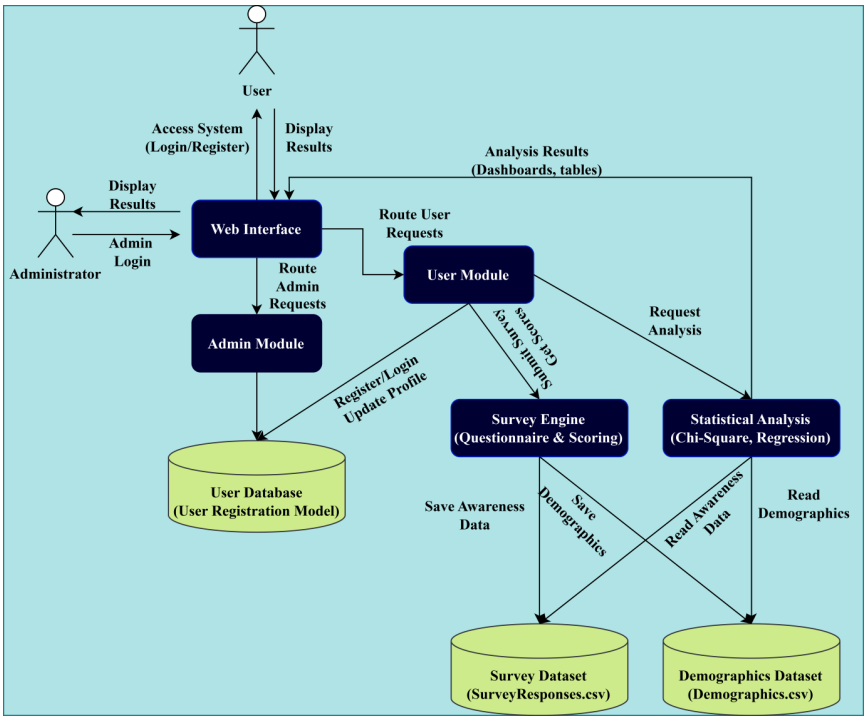

Fig. 1: Graphical representation of the System Architecture

3) Survey Engine and Awareness Scoring Model: A standardized questionnaire with Likert-scale items arranged into four cybersecurity awareness dimensions serves as the system's primary analytical input:
   - Background Knowledge (BBB)
   - Awareness of Cybercrime (AAA)
   - Education Level (EEE)
   - Ability to Deal with Cybercrime (CCC)

   For every user u_i, a score vector is created by combining the responses:

$$S_i = [B_i, A_i, E_i, C_i]$$

   Every dimension score is calculated as:

$$X_i = \frac{1}{m_x} \sum_{j=1}^{m_x} r_{i,j}$$

   where, $X_i \in \{B_i, A_i, E_i, C_i\}$, m_x is the number of questions in that category, and $r_{i,j}$ is the Likert response value.

   The overall cybersecurity awareness score for user u_i is describes as:

$$W_i = \frac{B_i + A_i + E_i + C_i}{4}$$

   Users are categorized into Novice, Intermediate, and Advanced awareness levels based on predetermined thresholds, and the interface provides instant feedback.

4) Data Storage and Dataset Modeling: Structured datasets are used to store all approved survey responses to facilitate statistical consistency and longitudinal studies. We keep two key datasets:
   - Survey Dataset:

$$\mathrm{S} = \{(B_i + A_i + E_i + C_i)\}_{i=1}^{n}$$

   - Demographics Dataset:

$$\mathcal{D} = \{D_i\}_{i=1}^{n}$$

     Flexible cross-analysis while maintaining data integrity is enabled by separating awareness and demographic data.

5) Statistical Analysis Module: The analytical engine uses well-established statistical methods to find significant correlations between cyber readiness, awareness indicators, and demographics.
   - Chi-Square Association Analysis: In order to investigate correlations between categorical variables, including education level and exposure to cybercrime, the Chi-square statistic is calculated as follows:

$$X^2 = \sum_{k=1}^{K} \sum_{l=1}^{L} \frac{(O_{kl} - E_{kl})^2}{E_{kl}}$$

     where, $O_{kl}\ and E_{kl}$ define frequencies that were seen and anticipated, respectively. This test assesses whether demographic characteristics significantly influence the likelihood of victimization or cybersecurity knowledge.
   - Regression-Based Readiness Modeling: A multivariate linear regression model is used to measure the relationship between awareness factors and the capacity to combat cybercrime:

$$C_i = \beta_0 + \beta_1 B_i + \beta_2 A_i + \beta_3 E_i + e_i$$

where, β_0 is the intercept, β_1, β_2, β_3 are regression coefficients, and e_i defines

This model illustrates the relative importance of background, education, and awareness, and provides a predictive interpretation of cybersecurity readiness.

6) Administrative Control and Research Dashboard: Controlled involvement is ensured via the admin module, which permits user activation, deletion, and dataset supervision. Analytical dashboards that display aggregated results include:
    - Average awareness ratings by demography
    - Tables with cross-tabulation
    - Summaries of correlations
    - Results of regression

    These observations aid in the development of policies, scholarly research, and focused cybersecurity awareness campaigns.

The presented design transforms the cybersecurity awareness assessment from an unstructured activity into a verified analytical system. Evidence-based assessment of cyber readiness at the individual and community levels is made possible by the system's integration of controlled user engagement, standardized measurement, and statistical modeling within a modular framework. This design is research-focused, scalable, and ideal for regional policy analysis and institutional application.

A. Deployment Architecture and Discussion

The architecture of the system is designed in a layer-based web architecture with the client, server, business logic, and data storage clearly separate. This is the best architecture for the analytical cybersecurity awareness system since it is easier to maintain, scalable, and modularized. The client layer is designed in such a way that the user will use the application using a normal web browser. The client layer is designed using HTML and CSS for simplicity, with the sole purpose of user interaction. No complex calculations or data storage will be performed in the client layer. The user interactions will then be sent securely to the server in the form of HTTP requests. The web server layer is designed using the Django Development Server. This is the default web server in Django for testing and local deployment. It acts as the mediator between the client layer and the business logic layer. The Django Development Server will receive the HTTP requests from the client layer and forward them to the appropriate components of the application using the URL dispatcher. The application can then be hosted using other servers such as Nginx or Apache without interfering with the business logic.

However, the core element of the deployment is the application server layer, which is implemented using a project named Security Awareness Level, implemented using the Django framework. The application server layer is divided into three main modules:

- User Module: The module is responsible for user authentication, user profiles, and access control, such that the participation and the results of the survey are restricted to authorized personnel.
- Admin Module: The module is used to provide administrative access, such that the entire system is well-managed and controlled, and all the operations are carried out in the best manner possible.

- Survey and Analysis Logic Module: The module is used to create, store, and analyze the cybersecurity awareness level surveys, such that the knowledge, practices, and attitudes of the users are assessed and evaluated through the analysis of the surveys.

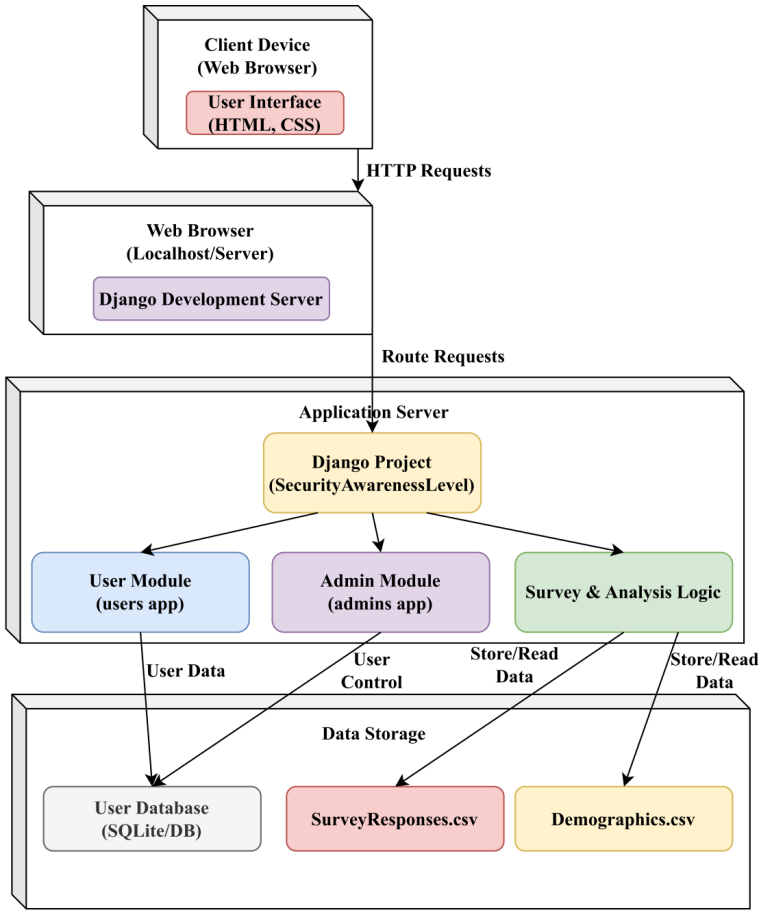

Fig. 2: Deployment architecture diagram

The application server interacts with the data layer through structured reading and writing, which ensures the integrity and consistency of the data. The data layer is implemented using a database, which is a SQLite database, and the data is stored in a structured CSV file, named SurveyResponses.csv and Demographics.csv.

IV. SYSTEM REQUIREMENTS AND ANALYSIS

The experimental setup for the proposed Cyber Security Awareness Level Assessment System was designed to provide a controlled, reliable, and reproducible environment for data collection, processing, and statistical analysis. The system was implemented as a web-based application and evaluated using a standardized hardware–software configuration to ensure consistent performance during experimentation. All experiments were conducted on a standalone computing system equipped with an Intel Core i9 processor, 32 GB RAM, and 1 TB storage, operating on a 64-bit Windows 10 platform. This hardware configuration was sufficient to support concurrent user interactions, server-side request handling, and computationally intensive statistical analysis without performance bottlenecks.

The software environment consisted of Python as the primary programming language and Django as the web application framework. The frontend interface was developed using HTML, CSS, and Bootstrap, enabling user-friendly interaction and efficient data input. Survey responses were stored in structured formats using SQLite and CSV files, ensuring ease of data management and reproducibility of results. Data preprocessing and statistical computations were performed using standard Python libraries, including Pandas, NumPy, and Statsmodels. User interaction and system evaluation were carried out using a modern web browser, preferably Google Chrome.

During experimentation, users accessed the system through a web interface to submit cybersecurity awareness survey responses. The collected data were validated, preprocessed, and stored securely. Statistical analyses, including Chi-square tests and regression analysis, were then applied to examine the relationships between background knowledge, education level, awareness of cybercrime, and the ability to deal with cybercrime. The results were generated dynamically and presented through the system interface for interpretation. This unified experimental setup ensured consistency in data collection, accuracy in statistical analysis, and repeatability of results. The use of open-source technologies and standardized hardware–software resources makes the proposed system scalable and suitable for further academic research and real-world deployment.

Dataset Description

The study has been informed by both new and existing data to be grounded in reality. On the ground, the study has been informed by primary data collected through a structured survey via Google Forms. The study has been conducted in a way that allows mapping of who the respondents are, what they know, what they think, and what they do in the domain of cybersecurity. Through a structured survey via Google Forms, it has been possible to obtain responses from a wide range of people. The study has obtained a total of 284 valid responses from the adult population aged 18 and over in Central India. For secondary data, the study has been informed by a literature search. The study has tapped into the existing research articles available in the online journal database J-Gate. The study has been grounded in the existing literature to stay in touch with the latest thinking in cybersecurity. For the study, the respondents in the Central region of India have been targeted. Judgmental sampling has been used to obtain the required data for the study. Using the sampling technique, it has been possible to obtain informed, meaningful data from respondents with diverse educational backgrounds.

Analysis of Data and Results

The analysis was carried out using 284 genuine replies gathered from respondents living in Central India. For statistical analysis, IBM SPSS Statistics Version 29 was used.

- Reliability Analysis: To assess the internal consistency of the survey instrument, Cronbach's Alpha reliability test was performed.

Table 1: Reliability Statistics Analysis

Measure	Value
Cronbach's Alpha	0.67
Number of Items	12

For exploratory and social scientific research, an adequate degree of internal consistency is indicated by the obtained Cronbach's alpha value of 0.67. A reliability score of 0.67 is regarded as adequate for perception-based and awareness-related investigations, however values nearer 0.7 or higher are preferable. This demonstrates that the survey items accurately assess the constructs being studied and that the dataset is appropriate for additional inferential statistical analysis.

- ANOVA Test: The association between professional experience and academic background in cybercrime victimization was examined using a Chi-square test.

Table 2: ANOVA Test Results Analysis

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	31.52	3	10.51	27.98	0.000
Residual	107.35	280	0.38		
Total	138.87	283			

The results of the ANOVA demonstrate that the regression model fits the data well, as evidenced by the statistically significant F-value ($F = 27.98$, $p < 0.05$). This demonstrates that the dependent variable is significantly predicted by the chosen independent factors.

- Regression Coefficients:

Table 3: Regression Coefficients Results Analysis

Variable	B	Std. Error	Beta	t	Sig.
Constant	0.332	0.061	—	5.44	0.000
Level of Background	0.299	0.047	0.281	6.36	0.000
Awareness about Cybercrime	0.387	0.052	0.341	7.44	0.000
Education Level	0.220	0.049	0.213	4.49	0.000

All independent variables show statistically significant positive relationships with the dependent variable ($p < 0.05$). Among them, awareness of cybercrime has the strongest influence, followed by background and education level**.**

The regression equation derived from the coefficients is:

Ability to Deal with Cybercrime=0.332+0.299(Level of Background)+0.387(Cybercrime Awareness)+0.220(Education Level)

This equation highlights the critical role of awareness and education in enhancing individuals' ability to respond effectively to cyber threats.

The report offers empirical data on cybercrime vulnerability and cybersecurity awareness in India's central region. The results show that younger people make up the most vulnerable and digitally active population, especially those aged 18 to 25. The survey tool is reliable and appropriate for inferential analysis, as indicated by the reliability analysis.

V. CONCLUSION

The present research has proposed a structured approach to the assessment of cybersecurity awareness, knowledge, and response capacity within individuals in Central India. The use of measurement theory and statistical modeling has enabled the quantification of subjective human awareness factors as objective cybersecurity readiness measures. The reliability test has confirmed the proposed approach, which has proven the acceptability of the proposed survey tool in terms of internal consistency. The use of regression modeling has proven the significant role played by cybercrime awareness, knowledge, and education levels in determining an individual's capacity to respond to cyber attacks. Among the factors, cybercrime awareness has been found to play a significant role in determining an individual's capacity to respond to cyber attacks. The development of the Cyber Security Awareness Level Assessment System has enhanced the present research, which has enabled the quantification of awareness evaluation through a web-based analytical system. The present research has proven the significant role played by awareness and education in determining cybersecurity readiness and mitigating human-based cybersecurity vulnerabilities. The proposed approach has the potential to be used as a research tool and has the potential to be used in the implementation phase.

REFERENCES

1. Ravichandran, R., Singh, S., & Sasikala, P. (2025). Exploring school teachers' cybersecurity awareness, experiences, and practices in the digital age. *Journal of Cybersecurity Education, Research and Practice, 2025*(1).
2. Panjani, H., & Mudgal, A. (2025). A study of cyber safety awareness among students and educational initiatives. *Indian Journal of Educational Technology, 7*(2), 246–256.
3. Sawale, P. T. (2025). Cybersecurity awareness and digital safety practices among secondary school teachers in urban and rural areas of Nashik. *Journal of Informatics Education and Research, 5*(2).
4. Bharad, B. H., & Sharma, K. B. (2025). Cybercrime awareness and its implications for digital transactions: A study among school educators in Ahmedabad City. *Sachetas*.
5. Verma, V., & Pawar, J. (2025). Assessment of students' cybersecurity awareness and strategies to safeguard against cyber threats. *Journal of Advanced Zoology*.
6. Roy, A., G., N., & Mukherjee, S. (2025). *ShieldUp!: Inoculating users against online scams using a game-based intervention* (arXiv Preprint). arXiv.
7. Rahartomo, A., Ghaleb, A. T. A., & Ghafari, M. (2025). *Phishing awareness via game-based learning* (arXiv Preprint). arXiv.
8. Toth, R., Dubniczky, R. A., Limonova, O., & Tihanyi, N. (2025). *Sustaining cyber awareness: The long-term impact of continuous phishing training and emotional triggers* (arXiv Preprint). arXiv.
9. Economic Times CISO. (2025, June 16). *India's education sector faces alarming surge in cyberattacks: 8,487 weekly threats uncovered*.
10. Rana, M. K. (2025, October 11). *Cybersecurity awareness among students in India—A 2025 report by BharatSec*. BharatSec.
11. McGregor, R., Reaiche, C., Boyle, S., & de Zubielqui, G. C. (2025). Consumer perceptions of personal cyber awareness, knowledge, and risk. *Journal of Cybersecurity, 11*(1), tyaf029.
12. Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: Insights from the health belief model. *Journal of Cybersecurity, 11*(1), tyaf034.
13. Rohan, R., Chutimaskul, W., Roy, R., Hautamäki, J., Funilkul, S., & Pal, D. (2025). Developing a scale for measuring the information security awareness of stakeholders in higher education institutions. *Education and Information Technologies*, 1–65.
14. Arpaci, I., Aslan, O., & Oner, I. E. (2025). Cybersecurity Awareness Scale (CSAS) for social media users: Development, validity and reliability study. *Information Development*.

15. Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: Implications for educational interventions. *Journal of Computers in Education, 12*(4), 1283–1305.
16. Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Arsenyan, A. (2025). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and fsQCA analysis. *Computers & Security, 150*, 104276.
17. Taherdoost, H. (2024). Towards an innovative model for cybersecurity awareness training. *Information, 15*(9), 512.
18. Abuabid, A. A. (2025). A data-driven approach to cybersecurity situational awareness: Insights from machine learning. *Journal of Innovative Digital Transformation*.
19. Ho, G., et al. (2025). Understanding the efficacy of phishing training in practice. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)* (pp. 37–54). IEEE.
20. Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security, 132*, 103364.
21. Ahmed, S. T., Kaladevi, A. C., Shankar, A., & Alqahtani, F. (2025). Privacy enhanced edge-ai healthcare devices authentication: a federated learning approach. *IEEE Transactions on Consumer Electronics*.
22. George, A. M., Rajan, K. T., Jambula, K. R., & Ahmed, S. T. (2025, August). Adaptive Firewall System to Predict Phishing Websites using Machine Learning Model. In *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)* (pp. 1-6). IEEE.
23. Fathima, A. S., Basha, S. M., Ahmed, S. T., Khan, S. B., Asiri, F., Basheer, S., & Shukla, M. (2025). Empowering consumer healthcare through sensor-rich devices using federated learning for secure resource recommendation. *IEEE Transactions on Consumer Electronics*.