iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79916

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

AI-Powered Multilingual Adaptive Learning Platform for Cyber Safety Education

Prof. Lavanya Pamulaparty[1], Gouni Sahithi[2], Aavulaw Trishal[3], Komaravelli Vedharth[4]
[1]*Professor & Head, Department of Computer Engineering, Methodist College of Engineering and Technology, Abids, Hyderabad, Telangana, 500001, India*
[2,3,4]*Students, Department of Computer Engineering, Methodist College of Engineering and Technology, Abids, Hyderabad, Telangana, 500001, India*

Abstract: ***In this digital era, people spend significant time online, rendering them vulnerable to a variety of cyber threats such as phishing, online scams, and data abuse or exploitation, to name a few. Despite a fairly high uptake of the internet, there is a huge gap in any cyber security training that reflects, regionally specific, age specific and multilingual information and delivery, especially in rural and semi-urban settings - contexts that are least served. This research paper provides an overview of the current advancements in the field of AI-based adaptive learning and gamification product aimed at developing digital literacy and cyber safety knowledge. It also reflects on the newest developments in artificial intelligence, gamification and tailored e-learning tools for training for safety and draws out the strengths and challenges for each. Finally, it presents a conceptual framework for an AI-based multilingual adaptive learning system that provides engaging and accessible cyber safety capacity building for learners of all ages. The paper concludes by explaining how artificial intelligence and adaptive content delivery could fill the gap in cybersafety, and assist with safe internet learning across the users.***

Keywords: Artificial Intelligence (AI), Adaptive Learning, Cyber Safety, Digital Awareness, Gamification, Multilingual Education, Personalized Learning,

I. INTRODUCTION

The integration of Artificial Intelligence (AI) in language education has introduced transformative advancements in instructional design, learner engagement, and assessment methodologies[1]. The proposed application is related to providing information on cyber safety, and it will be a web application through which users will be able to learn about cyber safety in an easy and interactive manner. The user will be able to login, select their preferred language, and access various learning modules according to their age group and level of understanding. The application is related to providing information on cyber safety, and it has been developed in a simple manner so that anyone can use it without facing difficulties. It support multiple languages, such as English, Hindi, and Telugu, through which the user will be able to learn in their preferred language. The content will be provided in multiple formats, making it interesting for the user. Overall, this application helps users understand cyber threats better and learn how to stay safe online in a simple and effective way[2]. At the same time, online learning systems are becoming popular due to their flexible nature. With the increasing use of digital platforms, the need for secure systems and user awareness has become essential. Studies highlight the importance of data protection and secure communication mechanisms, emphasizing the need for effective cybersafety solutions [3], [4],[5]. This project integrates both of these fields to provide a system that will assist users in effectively learning about cyber threats. This project integrates various aspects of cybersecurity with the latest e-learning systems to ensure that users learn about the importance of safe online practices[6]. The system also utilizes various aspects of adaptive learning to ensure that users have a more efficient and user-friendly experience[7]. E-learners are becoming extremely popular in recent times due to the availability of opportunities to learn anywhere and anytime through the internet. Such e-learners offer flexible learning opportunities to people of different backgrounds and make their education easy and convenient for everyone. Moreover, e-learners also include options such as videos and quizzes to make the learning process easy for the users. However, e-learners generally adopt a general approach and do not consider individual needs for learning. Because of this, users may not fully understand the content or stay engaged for a long time. This shows the need for more advanced e-learning platforms that can provide personalized and interactive learning experiences. Social media has transformed the communication landscape, although this has been at the expense of imminent dangers. Given that social media is based on the notion of community and relationships, its very nature means that users are expected to trust in each other and interact. Unfortunately, uncontrolled trust and thoughtless interaction may lead to vulnerabilities, which are often exploited by hackers. The implementation of the proposed system is carried out using a web-based architecture where the frontend and backend work together to provide a smooth learning experience.

A rule-based decision engine is used to adapt content dynamically based on user responses. The user first selects the preferred language, after that the user registers and logs into the system, and creates the profile accordingly. The dashboard retrieves modules from the backend through REST APIs. When a user selects a module, the system loads content based on age group, difficulty level, and language using predefined rules. The quiz module is used to check the performance, user responses, calculates scores, and verifies whether the user meets the required threshold. If the user passes, the next level will be unlocked, otherwise, the user is allowed to retry the module. After completing all modules, a certificate is generated dynamically. All user progress and performance data will be stored and managed using backend and database.

II. LITERATURE SURVEY

Laczi, et al., discussed various cybersecurity awareness games and assess their effectiveness in enhancing users' knowledge and behavior [8]. This is a comparative analysis of various game-based learning strategies. The various approaches have been compared in terms of their engagement, usability, and effectiveness. This is in the context of interactive simulation and game-based environments in enhancing users' knowledge of cybersecurity threats such as phishing and scams. The various factors analyzed include users' motivation, retention, and experience. Comparative Analysis of Cybersecurity Awareness Games. The paper demonstrates the effectiveness of gamification in enhancing users' engagement and retention compared to other forms of learning. However, there is a challenge in ensuring the usability of the games for various users.

S. Sengupta, et al., discussed the various aspects of adaptive learning in cybersecurity education and its applications[9]. The paper also discusses the role of adaptive learning in promoting cybersecurity awareness. The paper evaluates the different models of adaptive learning and their efficiency. Empowering Cybersecurity Education: A Review of Adaptive Learning Paradigms and Practical Implications. In the paper, it is clear that the use of adaptive learning in cybersecurity education has a number of benefits, including the retention of knowledge and increased engagement of users by providing customized content. However, there are drawbacks to the use of adaptive learning in cybersecurity education, including its complexity and the need to ensure data security and develop effective AI systems.

S. Kumar, et al., explored the level of cybersecurity awareness and digital literacy among the population in India[10]. The paper will address the effects of the increased use of technology and the related risks that arise because of the lack of awareness. The analysis will include the gaps in knowledge, which is crucial in addressing the importance of educational campaigns. Cybersecurity Awareness and Digital Literacy in the Context of Digital India. The analysis indicates that the level of digital literacy is crucial in enhancing cybersecurity awareness. There is a disparity in education and technology, which creates a gap in the awareness campaign.

S. L. Burton, sought to integrate artificial intelligence and cybersecurity education through the development of adaptive frameworks[11]. This paper, however, focuses on the integration of artificial intelligence in the dynamic adaptation of the content of the material to be learned based on the performance and behavior of the users. The objective of this paper is to explore the role of intelligent tutoring systems and predictive analytics in the optimization of the learning process. Integrating Cybersecurity and Artificial Intelligence: Adaptive Frameworks for Future-Ready Education. This paper proves the efficiency of artificial intelligence in enhancing the learning process. However, the integration of artificial intelligence in the learning process is challenged by its high implementation costs and the ethical issues surrounding artificial intelligence decision-making.

L. Y. Tan, et al., examined the role of artificial intelligence-enabled adaptive learning platforms in education systems[12]. It also examines various artificial intelligence methods such as machine learning and data analytics used to improve the learning process. The paper is focused on the scalability, efficiency, and effectiveness of these platforms. Artificial Intelligence-Enabled Adaptive Learning Platforms: A Review. The findings of the paper revealed that artificial intelligence-based platforms improve learner engagement and outcomes considerably. However, concerns such as data privacy and algorithmic biases remain major barriers to their effective implementation.

A. Alshehri, focused on AI-Powered Adaptive Cybersecurity Awareness Training in industrial settings[13]. The paper highlights the importance of developing training programs that are unique to the sector. The paper also evaluates the capability of AI systems to identify user weaknesses and provide training accordingly. AI-Powered Adaptive Cybersecurity Awareness Training for the Industrial Sector. The research indicates that AI systems are efficient in training and cybersecurity awareness. However, it also indicates challenges in implementing AI systems.

A. Carreiro, et al., aimed to examine the effect of gamification on cybersecurity awareness among healthcare professionals[14]. It seeks to understand how gamification learning improves engagement and knowledge retention among critical industries dealing with sensitive information. The paper assesses various gamification methods and their efficiency. The Use of Gamification on

Cybersecurity Awareness of Healthcare Professionals. The findings indicate that gamification improves engagement and learning outcomes, but challenges remain a significant concern.

A. K. Gwenhure, et al., focused on systematic review of the gamification techniques applied in the promotion of cybersecurity awareness among non-IT professionals[15]. The paper seeks to identify the best practices and challenges in the application of gamification. The research focuses on the accessibility, usability, and effectiveness of the gamified learning. Gamification of Cybersecurity Awareness for Non-IT Professionals. The findings of the research indicate that gamification makes it easy for non-technical users to comprehend cybersecurity concepts. The limitations include the lack of standardization and the inability to measure the long-term effectiveness.

A. L. Nkuna, et al., explained that the language used in the teaching of cybersecurity is of great importance to the students[16]. When a lesson is given in a language that a student is familiar with or his or her native language, the student understands the lesson better. According to the study, language has a big impact on how well a student understands the topic of online safety and dangers. The study also showed that when a lesson is easy to understand for a student, the student becomes more aware and confident. However, creating content in multiple languages is difficult and requires more time, effort, and resources, which is a major challenge.

B. M. T, R. Gagendra, et al., focused on the computer literacy level of Indian students and the digital divide[17]. It also discusses how a lack of access to technology and education impacts computer literacy and cybersecurity awareness. It also emphasizes the difference between urban and rural populations. Computer Literacy Competencies Among Indian Students: The Digital Divide. It shows that computer literacy must be improved to increase cybersecurity awareness. However, there are many problems to bridge the digital divide.

From the above studies, it has been observed that existing systems are focusing on individual aspects such as gamification, adaptive learning, or multilingual support. However, most of the existing systems are not focusing on all these aspects together. In addition, there are existing systems that lack user engagement or multilingual support. The proposed system will integrate all three aspects, namely adaptive learning, multilingual support, and gamification, to provide a more effective cyber safety education system.

III. METHODOLOGY

The proposed system is implemented using a structured approach where each component interacts to deliver adaptive cyber safety education efficiently. Cybersecurity awareness levels can vary significantly among both educators and students, which can impact the effectiveness of cybersecurity education. In the case of the proposed system, the frontend of the proposed system is designed by using simple web technologies to develop a user-friendly interface in which users can easily access various modules and attempt the quizzes without any difficulties. In the case of the proposed system, the backend of the proposed system is designed by implementing the main logic of the proposed system. The proposed system is designed in such a way that all the components of the proposed system work together to enable users to learn step by step. In general, the proposed system is designed in a simple and efficient way so that the proposed system is easy to implement and expandable for future use.

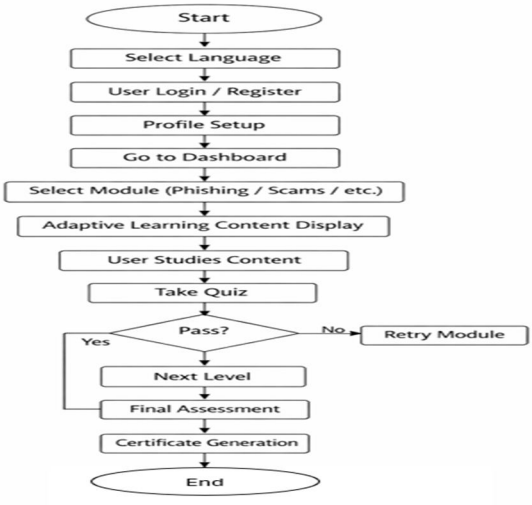


Figure 1:Flow of cybersafety platform

The proposed system is designed to adopt the adaptive learning approach for providing users with the benefits of personalized cyber safety education.

The working of the proposed system is designed in various steps:

1) First, the user selects the preferred language and logs in to the system. Based on user response the rule based decision engine adapts the content dynamically. Once the user logs in, they are directed to the dashboard where various modules are displayed.

2) The system then enables the user to choose a module, such as phishing, online scams, identity threats, or cyberbullying. Depending on the selected module, the system then provides the content to the user based on the age group, difficulty level, and language.

3) For the children, the system provides explanations and flashcards. For the youth, the system provides structured content and case studies. For the adults, the system provides scenarios to enhance their knowledge.

4) After the user is through with the content, they then have to undergo a quiz to assess their knowledge. The system then assesses the answers and determines the score. Once the user scores more than the required score, the next level is opened.

5) The entire process of the user is recorded by the system through local storage and backend APIs. Once the user is through with all the modules, they then undergo the final assessment. Once the user passes the assessment, the system generates a certificate.

6) The step-by-step process ensures the entire process of learning is easy and fun.

A. System Architecture

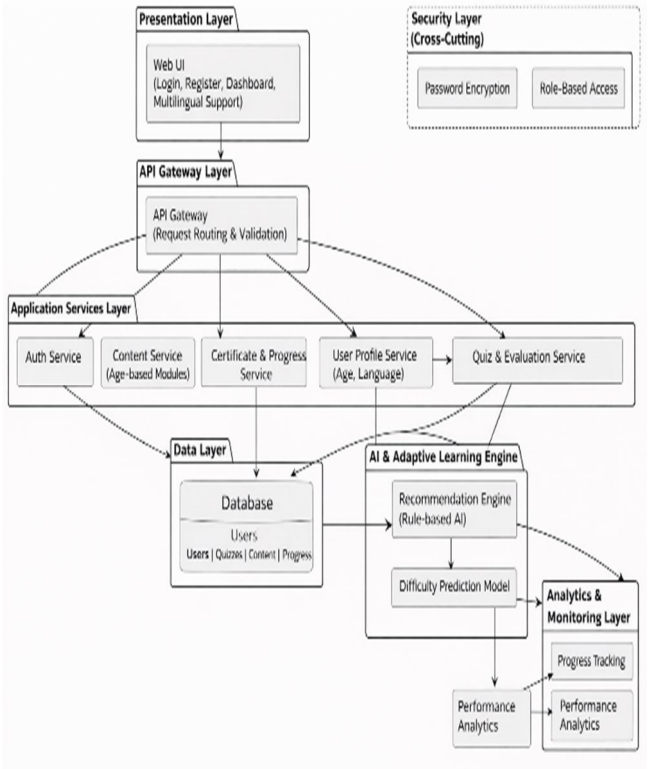


Figure 2:System Architecture of proposed cybersafety platform

B. System Architecture Layers

1) Presentation Layer: The proposed system has a layered architecture to ensure a clear separation of responsibilities and smooth interaction between components of the system. The proposed system has a layered architecture to ensure a clear separation of responsibilities and smooth interaction between components of the system.

2) API Gateway Layer: The API Gateway is the entry point for all the requests that come from the frontend of the application. This layer is responsible for routing the request to the appropriate backend services and for performing a simple validation of the request. This layer ensures that the interaction between the frontend and backend of the application is well organized and secure.

3) Application Service Layer: This layer contains the core functionalities of the proposed application. This layer contains a number of services: the Authentication Service handles user login and registration; the Content Service provides the content of the learning material according to age groups and modules chosen; the Certificate and Progress Service handles user progress and provides a certificate when a user has finished; the User Profile Service handles user information such as age and language; the Quiz and Evaluation Service handles quizzes and evaluates user results to determine whether they have passed or not. All these services operate collectively to ensure the complete learning experience.

4) Data Layer: The data layer holds all the necessary information for the system. This comprises the user's details, quiz, learning, and progress data. The database will be utilized for efficient retrieval of the data whenever necessary

5) AI & Adaptive Learning Layer: The system also comprises an adaptive learning component, which ensures the personalization of the learning experience for the users[21]. This has been implemented using the rule-based recommendation method. The system will be able to choose the necessary content for the users based on their factors such as age modules, and performance. In addition, the difficulty prediction mechanism will be utilized to ensure the content's difficulty level, neither too high for the users nor too low, thus enhancing the learning experience.

6) Analytics & Monitoring Layer: This layer ensures the tracking of the users' activity, including their performance. It tracks the users' progress for all the modules, including the quiz results. The data obtained from this layer will be utilized to ensure the understanding of the users' behavior, thus enhancing the overall system performance.

7) Security Layer: The security component is applicable for all the layers of the system. It comprises the password encryption method, thus enhancing the security for the users' credentials. The users will be restricted to the necessary features using the role-based access control method. This layer will be utilized for the maintenance of the privacy for the users.

IV. RESULTS AND DISCUSSION

The developed system was also tested with various users such as kids, students, and adults. Whereas, The results showed that the proposed concept of adaptive learning is helpful in understanding the concepts of cyber safety. The feature of multilingual support helped the users to increase the scope of the system. This feature is helpful for users who are not comfortable with the English language. The feature of gamification is also helpful in increasing the interest of users. Almost all the users completed the course and were able to retain the concepts. The integration of the frontend and backend of the system through the use of REST API is helpful in the smooth flow of the system. The proposed system is able to achieve its goal of developing an effective and user-friendly cyber safety education system.

From the results, it is clearly seen that the adaptive learning approach enhances the level of understanding among users by offering content suitable for various age groups. The users could complete their modules more efficiently than through traditional learning methods. The multilingual feature helped users to enhance their knowledge by allowing them to learn in their native language. The inclusion of gamification elements such as quizzes helped users to actively participate in completing their course. The proposed system works better than existing systems making it more easier and more effective for users to learn about cyber safety.

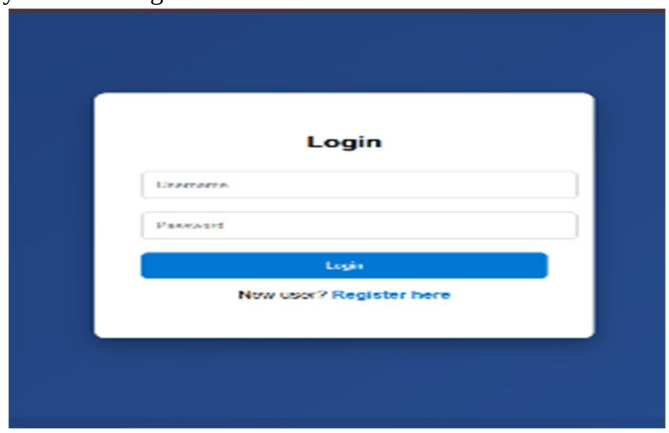


Figure 3:Login Page

The login interface allows users to securly access the system by entering the credintials. It provides a simple and user friendly design to ensure easy navigation for both new and exisitng users.

Figure 4:Profile Page

The profile creation interfacce collects basic user details. It also allows user to select an avatar making the system more interactive and engaging.

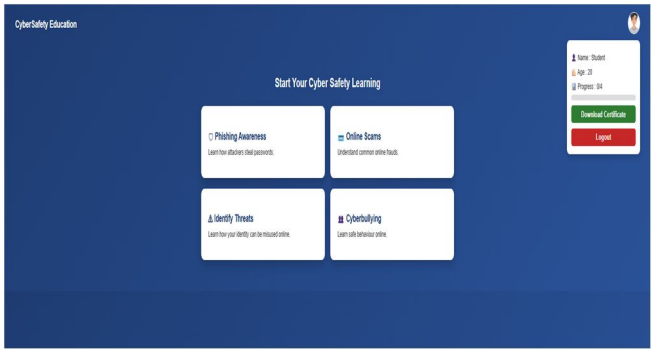


Figure 5:Dashboard

The dashboard provides users with different cyber safety learning modules and tracks the progress.

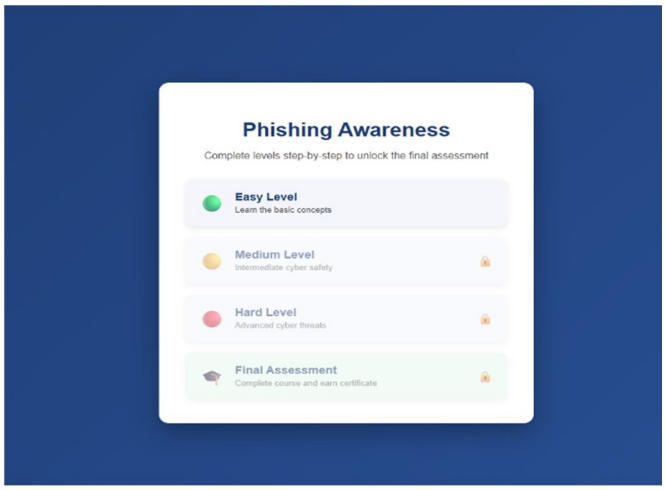


Figure 6:Module Page

The Modules are structured into multiple levels such as easy, medium and hard. Users must complete each level step by step to unlock the final assessment.

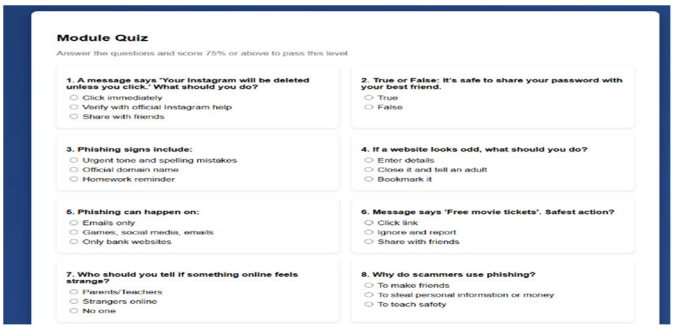


Figure 7:Quiz page

The module quiz evaluates the user understanding, and checks the user performance. User must achieve 75% score to earn certificate and enter into next module.

Figure 8: Certificate

The system generates a certificate if user passes the final quiz in each module. This feature motivate user to complete process.

Aspects	S. A. Laczi, S. I. Szabó, and V. Póser[5]	L. Y. Tan, S. Hu, and D. J. Yeo[9]	A. Carreiro, C. Silva, and M. Antunes [11]	**Proposed system**
Age group	There is specific age i.e(10-18)	Common for all users	No specific age	**Has 3 age groups i.e (5-15,16-30,30+)**
Multilingual	Only English	Only English	Only English	**Supports multiple languages (Telugu, Hindi, English)**
Target users	Only for young	Educational institutions, students	Health Professionals	**General users, learners**
Gamification	Fully gamified games	Not focused on games	Supports gamification	**Simple Interactive gamification elements**
Usability	Users not motivated to use	It is complex to use due to AI systems	Complex to use	**Simple and user friendly interface**
Application focus	Game based cybersecurity awareness	General education platform	Cybersecurity training in healthcare domain	**Cybersafety awareness for general users**

The comparison table indicates an analysis of existing systems and the proposed system with respect to various key evaluation criteria such as age group, multilingual support, target users, gamification method, usability, and focus of application. It is evident from the analysis of existing systems and the proposed system that existing systems are limited in scope. For example, the proposed system is applicable to a certain age group of 10-18 years, as indicated in the system proposed by Laczi et al. In contrast, the

proposed system is applicable to multiple age groups such as 5-15 years, 16-30 years, and 30+, which is an added advantage. With respect to multilingual support, it is evident from the analysis of existing systems and the proposed system that existing systems are limited in nature. All existing systems are only applicable to English-speaking users. In contrast, the proposed system is applicable to users speaking Telugu, Hindi, and English.

With respect to target users, it is evident from the analysis of existing systems and the proposed system that existing systems are limited in nature. For example, existing systems are applicable to certain user groups such as young learners, students, and healthcare providers. In contrast, the proposed system is applicable to general users and learners. As far as the gamification methods are concerned, the existing systems either heavily depend on the gamified games or do not consider them at all. However, the proposed system tries to strike a balance by incorporating interactive features such as flash cards, popups, and certificates that increase user engagement without making the system complicated.

Another area that the existing systems fail to address is the usability of the system. The proposed system provides ease of use for all kinds of users. The system is simple and user-friendly. Lastly, considering the application domain of the existing systems, they either deal with specific domains such as healthcare or are general educational systems. However, the proposed system deals with the domain of cybersafety awareness for general users. The proposed system addresses the needs of the real world and is quite relevant in the current scenario. From the above discussion, it is quite evident that the proposed system outperforms the existing systems in terms of accessibility, usability, and flexibility. Therefore, the proposed system is more appropriate for creating awareness about cybersafety.

V. CONCLUSION

The project seeks to create a cyber safety education system that will be used by users to learn about online security threats like phishing, scams, and cyberbullying through an interactive and user-friendly interface. The system is appropriate for all ages and three different languages, and it gives users a personalized experience, as well as tracking their activities. The system also tests the users through a quiz, allowing them to be tested on their performance. The system is highly effective and secure.

Overall, the system is effective, accessible, and practical for promoting cybersafety awareness among users

VI. FUTURE ENHANCEMENT

Despite In the future, we can also add AI and ML to make the recommendations for the content smarter rather than depending on a set of rules. We can also add real-time threat detection and simulations for users to practice their skills in detecting phishing sites and fake websites. We can also add more languages to make it easy for people to use the application. We can also add a mobile app for users to be able to learn anywhere and anytime they want. We can also add real-world cybersecurity data and tools for users to be able to practice their skills. We can also add analytics for tracking user progress and cloud for smooth operation of the application even for a large number of users.

REFERENCES

[1] A. Ezzaim, A. Dahbi, A. Aqqal et al., “AI-based learning style detection in adaptive learning systems: A systematic literature review,” Journal of Computer Education, vol. 12, pp. 731–769, 2025. doi: 10.1007/s40692-024-00328-9.

[2] Mangipudi, Mrs Sharada, P. SureshVerra, and M. Srinivasa Rao. "Pragmatic Approach for Financial Networking System Using Cyber Physical Systems Through Advanced Data Mining Concepts."

[3] Pamulaparty, Lavanya, T. Praveen Kumar, and P. V. Varma. "A Survey: Security Perspectives of ORACLE and IBM-DB2 Databases." International Journal of Scientific and Research Publications (2013): 272.

[4] Josphineleela R, Pellakuri V, Thanuja R, Moses D. Secure Internet of Thing based data communication in blockchain model using novel teaching-learning optimized fuzzy approach. Trans Emerging Tel Tech. 2023;34(7):e4793. doi: 10.1002/ett.4793

[5] F. Ben Salamah, M. A. Palomino, M. J. Craven, M. Papadaki, and S. Furnell, “An adaptive cybersecurity training framework for the education of social media users at work,” Applied Sciences, vol. 13, no. 17, article 9595, 2023, doi: 10.3390/app13179595.

[6] F. Tazi, S. Shrestha, and S. Das, “Cybersecurity, safety, and privacy concerns of student support structure for information and communication technologies in online education,” Journal of Computing and Information Technology, 2023.

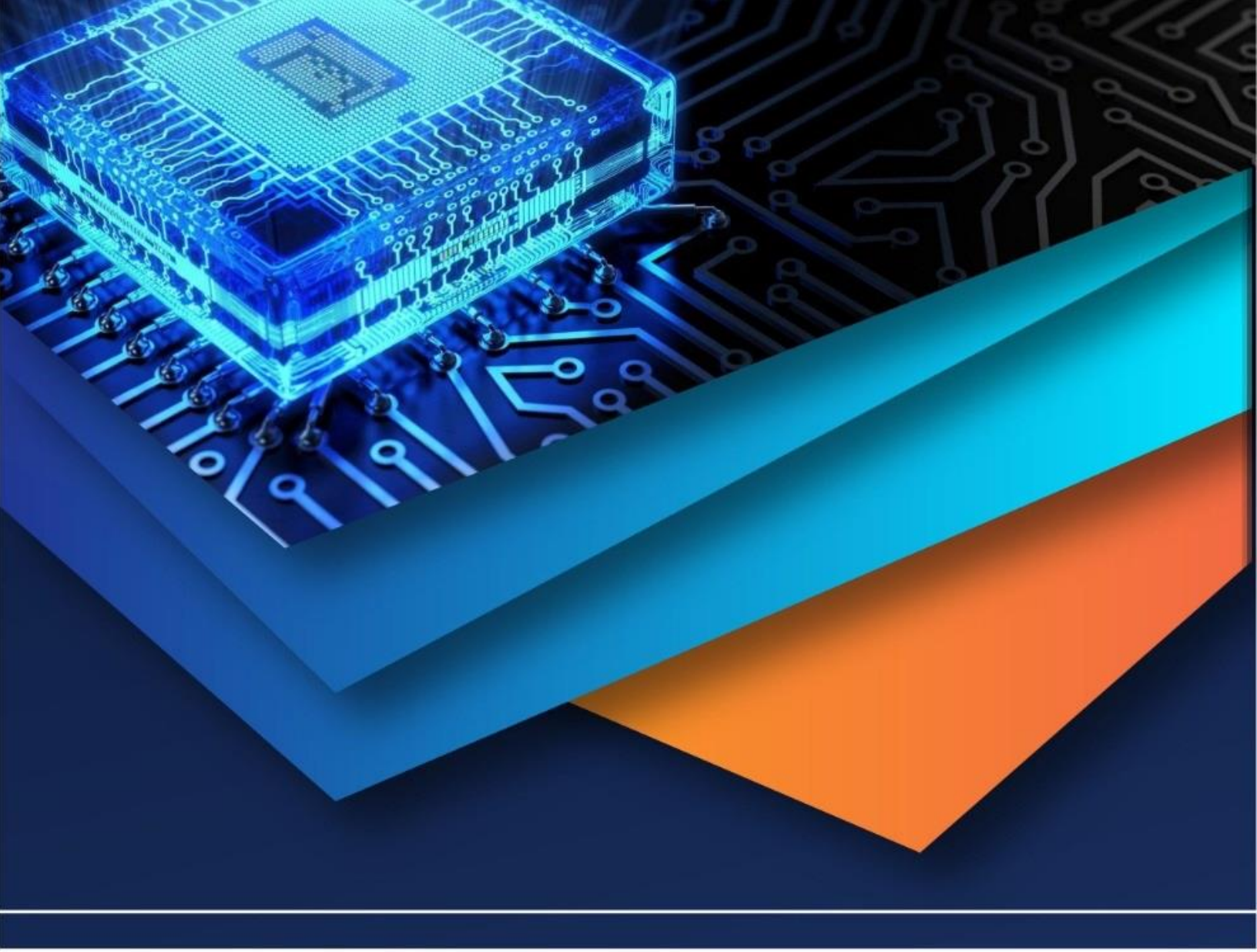
[7] C. Koukaras, P. Koukaras, D. Ioannidis, and S. G. Stavrinides, “AI-Driven Telecommunications for Smart Classrooms: Transforming Education Through Personalized Learning and Secure Networks,” 2025.

[8] S. A. Laczi, S. I. Szabó, and V. Póser, “Comparative Analysis of Cybersecurity Awareness Games,” in Proc. 2025 IEEE 19th Int. Symp. on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2025, pp. 93–97. doi: 10.1109/SACI66288.2025.11030134.

[9] S. Sengupta, U. Varma, and T. Islam, “Empowering Cybersecurity Education: A Review of Adaptive Learning Paradigms and Practical Implications,” in Proc. 10th Int. Symp. on End-User Development (IS-EUD), Munich, Germany, Jun. 2025.

[10] S. Kumar and G. Bansal, “Cybersecurity awareness and digital literacy in the context of digital India,” All Research Journal, vol. 11, no. 4, 2025. doi: 10.22271/allresearch.2025.v11.i4f.12568.

[11] S. L. Burton, "Integrating Cybersecurity and Artificial Intelligence: Adaptive Frameworks for Future-Ready Education," Embry-Riddle Aeronautical University, 2025.
[12] L. Y. Tan, S. Hu, and D. J. Yeo, "Artificial Intelligence-Enabled Adaptive Learning Platforms: A Review," Computers and Education: Artificial Intelligence, vol. 9, 2025, Art. no. 100429. doi: 10.1016/j.caeai.2025.100429.
[13] A. Alshehri, "AI-Powered Adaptive Cybersecurity Awareness Training for the Industrial Sector," Int. J. Intelligent Systems and Applications in Engineering, vol. 12, no. 4, pp. 5493–5505, 2024. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/7400
[14] A. Carreiro, C. Silva, and M. Antunes, "The use of gamification on cybersecurity awareness of healthcare professionals," Procedia Computer Science, 2024. doi: 10.1016/j.procs.2024.06.202.
[15] A. K. Gwenhure and F. S. Rahayu, "Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review," Int. J. Serious Games, vol. 11, no. 1, 2024. doi: 10.17083/ijsg.v11i1.719.
[16] A. L. Nkuna and E. Kritzinger, "Language as a Moderating Factor in Cyber-Safety Awareness Among School Learners in South Africa: Systematic Literature Review," in Communications in Computer and Information Science, 2024. doi: 10.1007/978-3-031-48930-3_34.
[17] B. M. T, R. Gagendra, and B. T. Sampath Kumar, "Computer literacy competencies among Indian students: The digital divide," Asian Education and Development Studies, vol. 3, no. 3, 2014. doi: 10.1108/AEDS-03-2014-0007.
[18] D. Ondrušková and R. Pospíšil, "The good practices for implementation of cyber security education for school children," Contemporary Educational Technology, vol. 15, no. 3, article ep435, 2023, doi: 10.30935/cedtech/13253



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY