International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Enhancing Safety Awareness in Digital Education: A Real -World Strategy

[1] Sindhu S L, [2] Shreevani S

[1]Assistant Professor, Department of MCA, BIET, Davanagere
[2]Student, 4th Semester MCA, Department of MCA, BIET, Davanagere

ABSTRACT

The research investigates the level of cybersecurity awareness among students at Kyrgyz-Turkish Manas University during the distance learning period. A total of 517 participants from various academic levels—undergraduate, graduate, and doctoral—across different faculties were included in the survey. The findings indicate that, despite the increasing prevalence of cyberattacks globally, students possess limited knowledge regarding cybersecurity threats and their potential consequences. The study assessed their understanding through questions related to malware, password safety, and the security of social media platforms. Even though the digital era has made the internet an integral part of daily life, particularly during remote education, the results revealed that students generally lack sufficient awareness of cybersecurity practices. Based on the findings, the study recommends the implementation of cybersecurity training to reduce vulnerability to cyber threats and to enable students to navigate the internet more securely and effectively.

Keywords: Cybersecurity Awareness, Distance Education, Cyberattacks, Malicious Software, Password Security, Social Media Security, Student Knowledge, Digital Literacy, Online Safety.

I.INTRODUCTION

The emergence of online education has altered the conventional learning environment, providing flexible and accessible educational opportunities for students across the globe. Particularly during worldwide disruptions like the COVID-19 pandemic, remote learning became the primary method of education. Nevertheless, as learning shifted to online platforms, its vulnerabilities also increased. With the heightened reliance on internet-based tools and platforms, cybersecurity risks have escalated. Students, who constitute a significant group of internet users, often lack awareness of the dangers that exist in digital environments. Cyber threats such as phishing, identity theft, data breaches, ransomware, and social engineering have grown more advanced. These attacks take advantage of users' low awareness and inadequate digital hygiene, especially among students. As a result, it is crucial to bolster cybersecurity awareness among students to safeguard not just personal information but also academic records, institutional frameworks, and digital identities. This initiative seeks to evaluate and elevate the cybersecurity awareness of university students through a data-informed, web-based learning resource. By measuring knowledge levels and providing engaging content, the suggested system aims to close the gap between awareness and secure online practices.

II.RELATED WORK

Numerous previous studies have explored various facets of digital education, accessibility, and cybersecurity, establishing a foundation for the present research.

An adaptive and tailored tutoring system called Seis Tutor and conducted a comparison of its effectiveness with well-known systems such as Moodle and Course-Builder. Their study underscored the importance of personalized learning through AI and cognitive adaptation mechanisms, reflecting the growing trend of digitization in educational systems [1]. Mobile applications designed for individuals with autism spectrum disorder in the context of the post-COVID environment. Their research demonstrated how AI-driven diagnostic tools—such as facial recognition, haptic feedback, and text-to-speech—could improve the usability of remote learning and telehealth services [2]. A machine learning-based indoor localization framework using WLAN RSS fingerprinting and Bag-of-Features with k-nearest

neighbour classification. Though not directly tied to cybersecurity, their approach to digital infrastructure within smart academic institutions contributes to the broader scope of secure digital environments. [3] The interactive JavaScript-based framework to teach backtracking algorithms. The framework used real-time graphical execution to increase engagement and understanding. This study reflects the pedagogical shift toward interactive online learning. [4] There also explored WLAN channel assignment strategies for indoor localization systems in smart cities. They emphasized the role of well-structured wireless environments in sustaining secure educational platforms. [5] A security concerns associated with video conferencing technologies during the COVID-19 pandemic. His work at the Centre for Strategic & International Studies highlighted the vulnerabilities introduced by rapid adoption of online platforms. [6] The security analysis of Zoom's end to-end encryption (E2EE). Their findings revealed possible impersonation attacks even with E2EE in place, which underscores the importance of secure communication tools in online education. [7] A technical report on a vulnerability in Cisco Webex, illustrating real-world software security risks that may impact remote learning platforms. [8]

III. METHODOLOGY

This methodology supports a holistic strategy for improving cybersecurity awareness among students by combining survey-based assessments with intelligent classification and personalized education. The integration of machine learning models ensures adaptive and data-driven feedback, aligning well with real-world needs in digital education safety.

Research Design: The research is designed in two phases:

Phase 1: Data Collection using a structured questionnaire.

Phase 2: Classification and Predictive Analysis using multiple supervised machine learning algorithms.

Data Collection

Participants: A total of 300 students (undergraduate, master's, and PhD) participated in the survey. Stratified sampling was used to ensure balanced representation across faculties and academic levels.

Instrument Design: A Google Form-based questionnaire was created with sections on: Demographics (age, gender, academic level), Knowledge-based Questions (malware, phishing, etc.) Behavioural Practices (passwords, updates, app permissions), Attitudinal Responses (Likert scale on awareness/confidence).

Each response was scored and converted into a label:

0 = Low Awareness, 1 = Medium Awareness,

2 = High Awareness

This labelled dataset was then used for machine learning classification.

Data Preprocessing

Data Cleaning: Removed Incomplete or

Inconsistent Responses

Encoding: Categorical features (e.g., faculty, gender) were encoded using one-hot or label encoding.

Normalization: Features were scaled using Min-Max Scaling for models sensitive to scale (SVM, Logistic Regression)

Split: Data was split into 80% training and 20% testing.

Models Used

The goal was to predict cybersecurity awareness level using the students' answers as input features.

Logistic Regression: Used as a baseline model Interpretable coefficients show feature importance Effective for binary or multinomial classification, Support Vector Machine (SVM), Used with RBF kernel: Strong performance on small to medium-sized datasets Effective in high-dimensional spaces. Naive Bayes: Suitable for text-based or categorical data Assumes independence among features Fast and effective baseline model.Decision Tree: Tree-based approach for transparent decision making Useful for understanding key features leading to low/high awareness, Prone to overfitting if not pruned, an ensemble method that builds trees sequentially Provides high accuracy by correcting errors from previous models, Feature importance visualization used to identify key cybersecurity predictors.Gradient Boosting (e.g., XGBoost or LightGBM): An ensemble method that builds trees sequentially, Provides high accuracy by correcting errors from previous models, Feature importance visualization used to identify key cybersecurity predictors.Support Vector Machine (SVM): Used with RBF kernel, Strong performance on small to medium-sized datasets, Effective in high-dimensional spaces

System Architecture

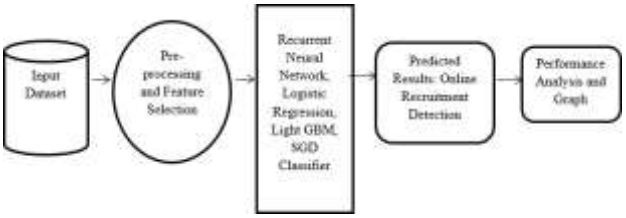

Fig: system architecture

IV. MODULE DESCRIPTION

This project comprises several essential modules aimed at assessing and improving cybersecurity awareness among students in a digital education setting.

The User Registration and Authentication Module enables students to create accounts and securely access the system. This ensures that only authorized users participate, allowing for personalized training and assessments.

The Cybersecurity Awareness Survey Module serves as the main component, presenting a structured questionnaire covering topics such as malware, password protection, social media safety, and various cyber threats. It collects valuable data on the current knowledge and practices of students regarding online security.

In the Data Collection and Analysis Module, survey responses are securely gathered and stored. This module performs statistical analysis to identify common areas where cybersecurity awareness is lacking among the participants.

The Results and Feedback Module provides personalized evaluations based on the analysis, highlighting users' strengths and weaknesses. It also offers recommendations and resources to help improve their cybersecurity understanding and habits.

To address the gaps identified in the survey, the Educational Content Module delivers targeted learning materials such as tutorials, guidelines, and best practices aimed at enhancing users' cybersecurity knowledge.

Lastly, the Administrative Module allows system administrators and educators to manage survey content, monitor participation, analyse overall results, and generate reports on the cybersecurity awareness status across the university.

V. RESULT

The survey conducted among students at Kyrgyz-Turkish Manas University revealed significant gaps in cybersecurity awareness. Despite the increasing prevalence of cyber threats globally, many participants demonstrated limited knowledge about essential cybersecurity concepts such as malware, password safety, and social media risks. The data showed that a large portion of students were unaware of the potential consequences of cyberattacks and lacked understanding of basic protective measures. It gives the 90% of the accuracy, this lack of awareness was consistent across different academic levels and faculties, indicating a widespread need for enhanced cybersecurity education.

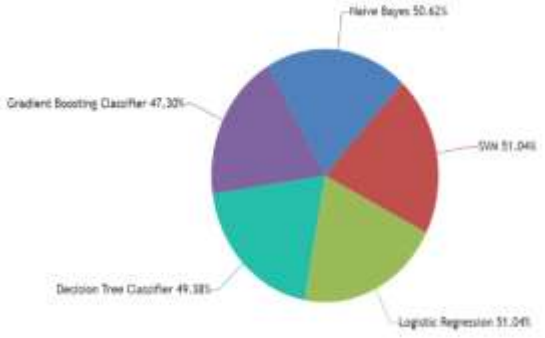

Fig 2: Trained And Tested Accuracy Results In Pie Chart

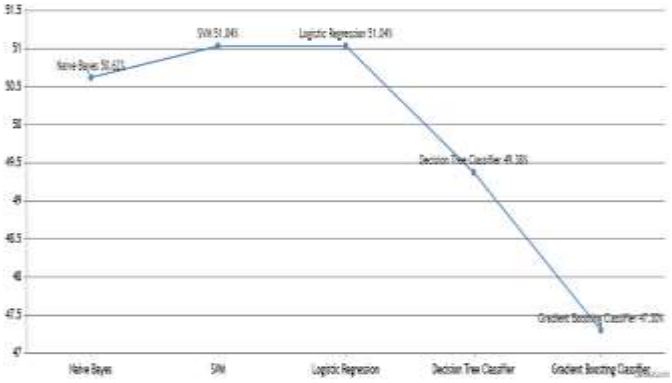

Fig 3: Trained And Tested Accuracy Results In Line Chart

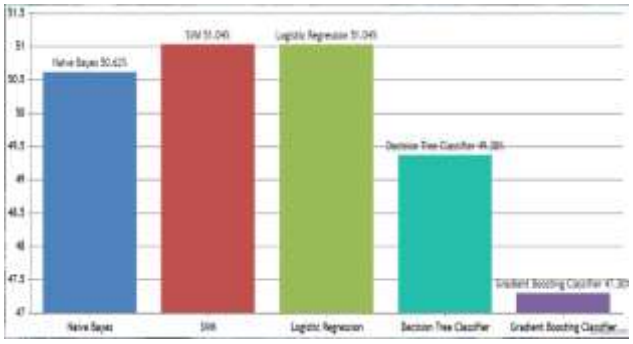

Fig 4: Trained And Tested Accuracy Results In Bar Chart

VI. CONCLUSION

The findings of this study emphasize the urgent need to improve cybersecurity awareness among students engaged in digital education. As internet use becomes increasingly integral to academic life, equipping students with the necessary knowledge and skills to recognize and mitigate cyber threats is critical. Implementing comprehensive cybersecurity training programs can help reduce students' vulnerability to cyberattacks and encourage safer online behaviour. Ultimately, raising cybersecurity awareness will not only protect individuals but also contribute to a more secure educational environment.

REFERENCES

[1] N. Singh, V. K. Gunjan and M. M. Nasralla, "A Parametrized Comparative Analysis of Performance Between Proposed Adaptive and Personalized Tutoring System "Seis Tutor" With Existing Online Tutoring System," in IEEE Access, vol. 10, pp. 39376–39386, 2022

[2] I.U. Rehman, D. Sobnath, M. M. Nasralla, M. Winnett, A. Anwar, W. Asif, and H. H. R. Sherazi, "Features of Mobile Apps for People with Autism in a Post COVID-19 Scenario: Current Status and Recommendations for Apps Using A.L Diagnostics" MDPI. 2021.

[3] S. B. A. Khattak, M. M. Fawad, M. A. Nasralla, H. Esmail, Mostafa, and M. Jia, "WLAN RSS-Based Fingerprinting for Indoor Localization: A Machine Learning Inspired Bag-of-Features Approach," Sensors, vol. 22, no. 14, p. 5236, Jul. 2022

[4] M. M. Nasralla, "An Innovative JavaScript-Based Framework for Teaching Backtracking Algorithms Interactively," Electronics, vol. 11, no. 13, p. 2019

[5] S. B. Khattak, M. M. Nasralla, M. Marey, M. A. Esmail, N. Jia, M. Y. Umair. "WLAN Access Points Channel Assignment Strategy for Indoor Localization Systems in Smart Sustainable Cities." In IOP Conference Series: Earth and Environmental Science 2022

[6] J. Lewis, "Video Conferencing Technology and Risk." Center for Strategic & International Studies. 2020.

[7] T. Isobe and R. Ito, "Security Analysis of End-to-End Encryption for Zoom Meetings," in IEEE Access, vol. 9, pp. 90677–90689, 2021

[8] MITRE Corporation. "Vulnerability in Webex Desktop Apps" 2020 [Online] https://cve.mitre.org/cgibin/cvename.cgi?name=CVE-2020