Cybersecurity Awareness Platform - An Interactive Training Module for Educating Users

Atchaya Varshini L[1], Dr. K. Thenmozhi[2]

[1]Department of Information Technology, Dr N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

[2]Professor, Department of Information Technology, Dr N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: ***People are now much more vulnerable to cyberthreats like phishing, malware, identity theft, ransomware, and social engineering attacks due to the quick rise in internet usage and digital services. Most of these attacks succeed not because of technical flaws but due to a lack of user awareness and unsafe online behaviours. Traditional awareness programs often rely on static content and lack user engagement, resulting in poor knowledge retention and limited behavioural change. This research proposes the design and implementation of a Cyber Security Awareness Platform that offers an interactive and engaging learning environment. The platform combines multimedia educational modules, real-time attack simulations, gamified quizzes, and performance analytics to improve users' understanding of cybersecurity threats and safe digital practices. Based on user performance and knowledge gaps, the system's personalised learning approach modifies training. Phishing detection, password security procedures, and general cyber hygiene have all significantly improved, according to an experimental evaluation conducted with a group of users. The proposed platform proves the effectiveness of experiential and gamified learning in enhancing cybersecurity awareness.***

Keywords: Cybersecurity awareness, phishing simulation, gamification, digital literacy, interactive learning, user education

1. Introduction

The widespread adoption of digital technologies has transformed modern society, enabling seamless communication, online transactions, cloud computing, and digital education. However, this rapid digitalisation has also created new opportunities for cybercriminals. Cyber attacks targeting individuals and organisations have increased in sophistication, frequency, and impact. Reports indicate that human error remains one of the main causes of successful cyber breaches.

Cybersecurity awareness is crucial for reducing risks by teaching users safe digital habits and threat detection. Sadly, many existing programs rely on lectures, manuals, or static training materials that do not effectively engage users. Consequently, users often forget important security practices and stay vulnerable to attacks.

To address this issue, this research proposes an interactive cybersecurity awareness platform that combines experiential learning, attack simulation, and gamification to enhance user engagement and knowledge retention. The platform aims to bridge the gap between theoretical knowledge and practical cybersecurity skills.

2. Literature Review

Current research on cybersecurity awareness mainly concentrates on policy-based training and organisational programs. Studies from the SANS Institute (2022) indicate that ongoing awareness initiatives decrease susceptibility to phishing, but these methods are mostly corporate-focused and lack adaptive learning features. Similarly, frameworks introduced by the National Institute of Standards and Technology (2021) offer best-practice guidelines but provide limited support for implementing interactive training platforms.

Recent research emphasises gamified and behaviour-driven learning models. Alotaibi et al. (2022) observed improved engagement and knowledge retention through gamification, while Bada and Nurse (2020) highlighted the importance of user motivation in awareness effectiveness. Nonetheless, scalability and personalisation continue to be significant hurdles.

Industry phishing simulation platforms like Cofense (2023) and KnowBe4 (2023) offer experiential learning but often operate as standalone commercial tools with limited customisation for academic purposes. Academic web-based awareness portals (Sharma et al., 2023; Li and Chen, 2022) incorporate multimedia learning but lack adaptive analytics and comprehensive simulation features.

Overall, the existing literature identifies gaps, including the absence of unified platforms that combine learning, simulation, and assessment, as well as limited personalisation and minimal focus on student users. To address these challenges, the proposed Cybersecurity Awareness Platform provides an interactive web-based training module that integrates multimedia content, phishing simulations, quizzes, and performance analytics to improve user engagement and practical cybersecurity awareness.

3. Proposed System

The proposed Cyber Security Awareness Platform is an interactive, web-based system designed to educate users about cybersecurity threats through structured learning, simulations, and assessments. The system combines authentication, content management, simulation-based training, automated evaluation, and performance tracking into a unified architecture. Its design ensures modularity, scalability, and effective user engagement.

DOI: https://dx.doi.org/10.21275/SR26311131159

1) *Modules of the Proposed System*

The system is divided into multiple functional modules to ensure scalability and maintainability.

a) **User Authentication Module:** This module manages secure registration and login processes using encrypted credentials and role-based access control.
b) **Learning Module:** Provides structured educational content on topics including phishing, malware, ransomware, and security threat.
c) **Simulation Module:** Offers interactive scenarios that mimic real cyber attacks, enabling users to practice threat detection.
d) **Quiz and Assessment Module:** Evaluates user understanding through quizzes and provides immediate feedback.
e) **Analytics Module:** Tracks user performance and generates detailed reports on awareness levels.
f) **Admin Module:** Allows administrators to manage content, monitor user progress, and generate reports.

2) *Workflow*

The overall workflow of the system follows a structured sequence:

a) **User Registration and Login:** The user registers by providing the required credentials. Upon successful login validation, access is granted based on role.
b) **Learning Phase:** The user accesses topic-based learning modules. Educational content is displayed from the database.
c) **Simulation Phase:** After learning, the user engages in simulated cyber threat scenarios. The system records responses and evaluates decision accuracy.
d) **Assessment Phase:** The user attempts a quiz related to the completed topic. The system automatically evaluates answers and calculates the score.
e) **Evaluation and Feedback:** Scores from simulations and quizzes are combined to generate a performance metric. Personalised feedback is provided.
f) **Progress Dashboard Update:** The system updates the user dashboard with completion status, scores, and improvement indicators.
g) **Admin Monitoring:** Administrators can review analytics and overall system usage statistics.

This workflow ensures a progressive learning model from theory to practice and evaluation.

3) *Methodology*

The development of the proposed system follows a structured Software Development Life Cycle (SDLC) approach.

a) **Requirement Analysis**
System requirements were identified based on cybersecurity awareness needs. Functional requirements include authentication, content delivery, simulation generation, and performance tracking. Non-functional requirements include usability, reliability, and security.

b) **System Design**
System architecture was designed using a layered approach. The database schema was developed using relational modelling. ER diagrams were used to define entity relationships such as User, Admin, Quiz, Simulation, and Score.

c) **Implementation**
The system was implemented using a web-based technology stack:
- **Frontend:** Developed for an interactive user interface and dashboard visualisation.
- **Backend:** Handles authentication logic, content management, simulation evaluation, and score calculation.
- **Database:** Stores user credentials, learning materials, quiz questions, and performance data.

d) Algorithm Design
Core algorithms include:
- Authentication validation logic
- Quiz answer verification algorithm
- Simulation decision evaluation algorithm
- Performance score computation logic

e) Testing
Functional, usability, and data validation testing were conducted to ensure system reliability. All modules were verified to process input correctly and generate accurate results. This structured methodology ensures systematic development and maintainability.

4. System Architecture

The proposed Cybersecurity Awareness Platform is designed with a modular, layered architecture in which the learning interface, simulation engine, and data analytics components operate independently yet communicate via secure APIs. This decoupled design improves scalability, enables easy content updates, and supports the integration of new cybersecurity training scenarios without affecting core system functionality.

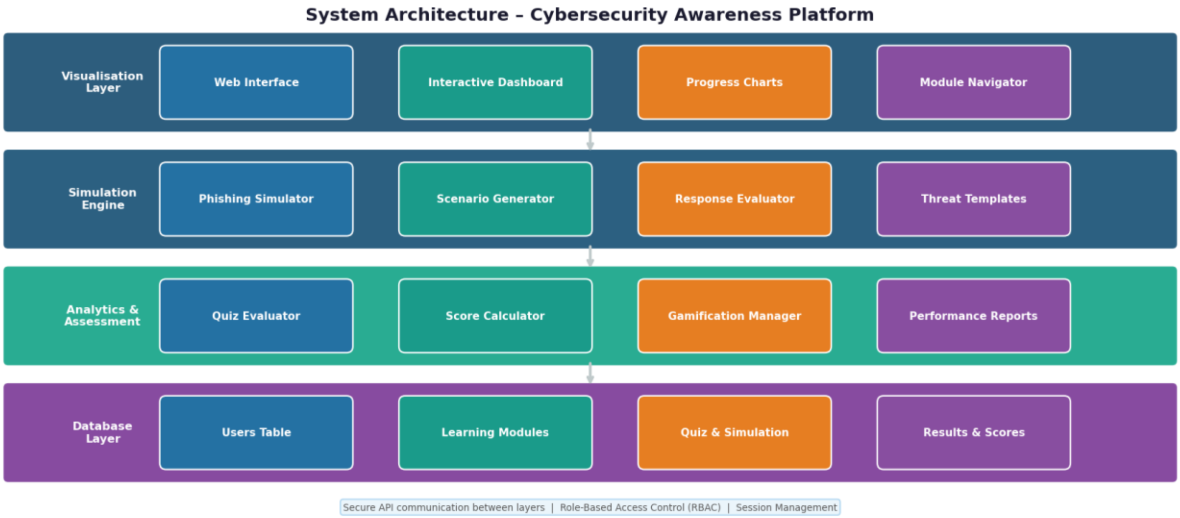

Figure 1: System Architecture of the Cybersecurity Awareness Platform

1) **Visualisation Layer: Web Interface & Interactive Learning Dashboard**

The visualisation layer provides an interactive web interface that delivers training content and supports user interaction. Unlike static awareness portals, the platform adopts responsive web technologies to dynamically render videos, infographics, simulations, and quiz interfaces.

This layer acts as the presentation framework through which users navigate modules, attempt simulations, and view progress dashboards. Content is loaded dynamically to reduce latency and ensure smooth learning experiences across devices. The dashboard also visualises performance metrics such as quiz scores, badge achievements, and module completion rates, enabling users to track improvements in awareness.

2) **Simulation Engine: Threat Emulation and Scenario Generation**

To convert theoretical knowledge into practical understanding, the system incorporates a simulation engine that generates realistic cyberattack scenarios. This module emulates phishing emails, weak-password detection, and social-engineering interactions using predefined templates and rule-based logic.

When users engage with simulation activities, the engine evaluates their responses in real time and records behavioural outcomes. This approach enables experiential learning by exposing users to controlled attack environments without compromising system security. The modular design also allows administrators to introduce new threat scenarios, ensuring adaptability to evolving cyber risks.

3) **Analytics and Assessment Engine: Performance Tracking & Feedback Mechanism**

The analytics engine is the core intelligence component of the platform, processing user interaction data and generating personalised feedback. Quiz attempts, simulation responses, and module engagement metrics are analysed to calculate awareness scores and identify knowledge gaps.

Gamification elements such as points, badges, and leaderboards are managed within this layer to encourage continuous participation. Additionally, administrators can access aggregated analytics through dashboards that highlight user progress, common mistakes, and training effectiveness. This data-driven feedback loop ensures continuous improvement of both learner performance and platform content.

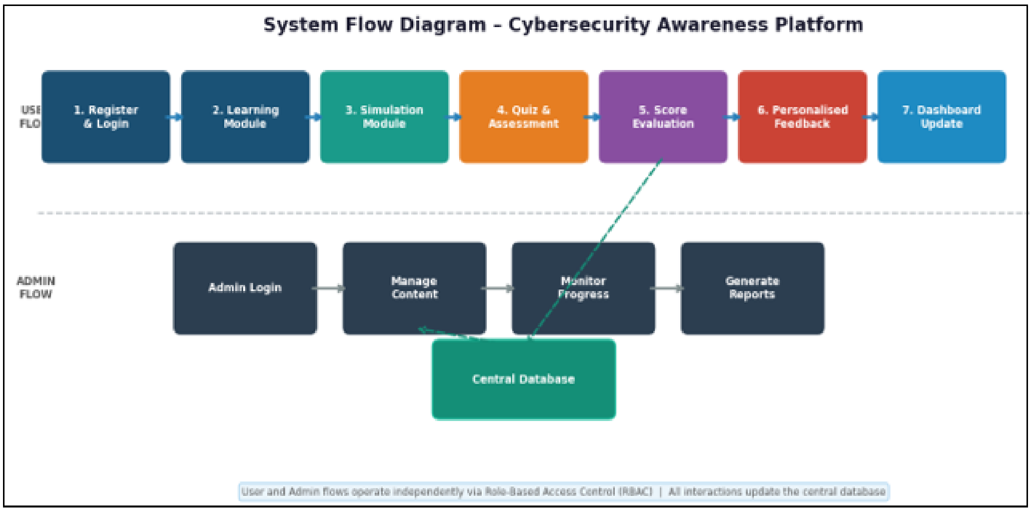

Figure 2: System Flow Diagram

5. System Implementation

1) Implementation Overview

The Cyber Security Awareness Platform was implemented as a web-based system designed to provide structured and interactive cybersecurity training. The implementation follows a modular architecture where user authentication, learning modules, simulation exercises, quizzes, and analytics operate as interconnected components. The system supports two primary roles: user and administrator. Users interact with training content and assessments, while administrators manage content and progress monitoring.

2) User Authentication Implementation

The system begins with user registration and login. During registration, users provide personal details such as name, email, and password. These details are stored securely in the database, with passwords encrypted. When users attempt to log in, authentication logic verifies credentials against stored data. Invalid login attempts trigger error messages and prevent unauthorised access. Successful authentication redirects users to the learning environment.

Implementation features include input validation for registration fields, password hashing for secure storage, session management to maintain login state, and role-based access control.

3) Learning Module Implementation

After authentication, users access the learning module, which provides structured cybersecurity training content. The module displays topics with module identifiers, titles, and descriptions stored in the database. Content is dynamically loaded to allow administrators to update materials without code modifications. Users can navigate through multiple cybersecurity topics, including phishing awareness, malware prevention, password safety, and social engineering defence. Completion of learning modules updates user progress records.

4) Simulation Module Implementation

After theoretical learning, users enter the simulation module, which replicates real-world cyberattack scenarios, such as phishing emails and fake websites. This module is implemented using predefined templates stored in the database. Users interact with simulated scenarios by identifying suspicious indicators. The system evaluates responses using rule-based logic and assigns scores based on correctness. Immediate feedback helps users understand mistakes and reinforces learning outcomes.

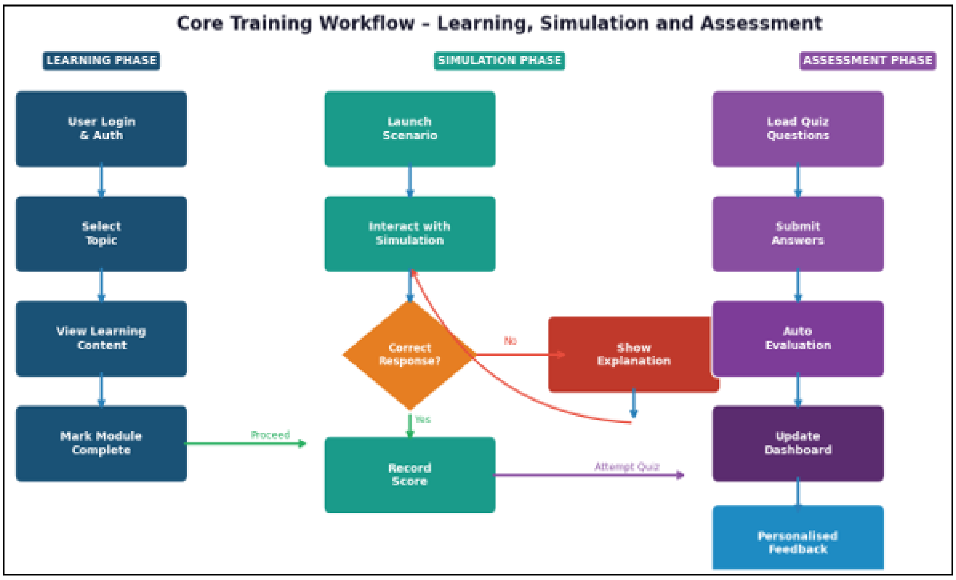

Figure 3: Core Training Workflow – Learning, Simulation and Assessment

5) Quiz Module Implementation

The quiz module assesses user understanding after simulation exercises. Questions are dynamically retrieved from the database and presented in multiple-choice format. The system supports randomised question selection to prevent memorisation. When submitted, the backend automatically evaluates answers, calculates scores, and stores results. Explanatory feedback is given for incorrect responses, helping reinforce knowledge.

6) Progress and Score Evaluation

The progress evaluation component combines data from learning, simulation, and quiz modules. The system computes an overall awareness score based on user performance across all activities. Evaluation criteria include module completion rate, simulation accuracy, and quiz performance. The resulting score indicates the user's awareness level and activates personalised feedback recommendations.

7) User Dashboard Implementation

The user dashboard acts as a central interface showing profile details, completed modules, quiz results, and awareness progress. Data is fetched from the database and displayed through charts and progress bars. This dashboard helps users track their learning achievements and spot areas that need improvement.

8) Admin Module Implementation

The admin workflow starts with a secure admin login. After authentication, administrators access the admin dashboard, which offers system management features including managing users, managing learning content and quiz questions, monitoring user progress and awareness levels, and generating performance reports. Administrative actions dynamically update database records, ensuring real-time system maintenance.

9) Database Implementation

The database supports multiple entities aligned with the system flow diagram. Key tables include the User table for authentication and profile data, the Learning module table for training content, the Simulation table for scenario templates, the Quiz table for questions and answers, and the Results table for scores and progress data. Relationships between these tables enable integrated evaluation and analytics.

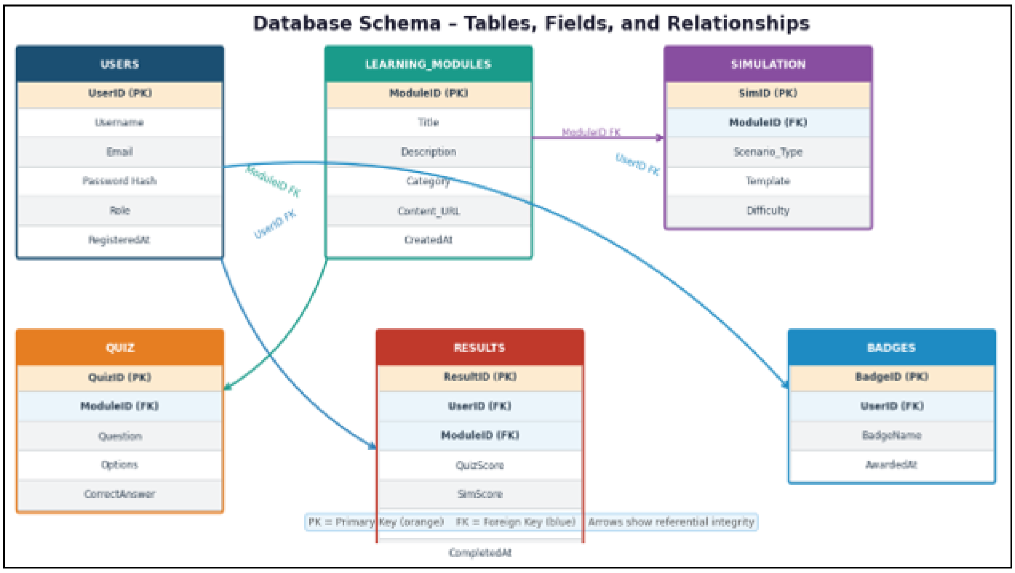

Figure 4: Database Schema – Tables, Fields, and Relationships

6. Performance Evaluation

The effectiveness of the proposed Cyber Security Awareness Platform was assessed through pre-training and post-training evaluations. Users engaged in learning modules, simulations, and quizzes, with their performance gauged by enhancements in awareness, engagement, and system responsiveness.

a) *Comparative Performance Table*

Table 1: Performance Comparison Before and After Training

Metric	Before Training	After Training (Proposed System)	Outcome
Phishing Detection Accuracy	42%	85%	Significant improvement in identifying malicious emails
Password Strength Level	Weak / Medium	Medium / Strong	Users adopted stronger password practices
Quiz Score Average	48%	88%	Increased knowledge retention
Simulation Success Rate	40%	82%	Improved decision-making in cyber attack scenarios
Module Completion Rate	55%	92%	Higher engagement due to gamification
Awareness Score (Overall)	45%	86%	Enhanced cybersecurity awareness
User Engagement Level	Moderate	High	Active participation in training activities
System Response Time	~2.1 sec	~1.4 sec	Faster and smoother user interaction

7. Output and Analysis

The evaluation results show that the proposed platform enhances cybersecurity awareness and user behaviour. Simulation-based training improves phishing detection accuracy, while gamification boosts engagement and module completion. Password feedback encourages stronger authentication habits, and improved quiz scores indicate better knowledge retention. Reduced response time further confirms an efficient system performance.

The results confirm that the integrated approach of combining multimedia learning, attack simulation, gamified assessment, and personalised feedback is significantly more effective than traditional static awareness programs. Users who completed the platform demonstrated measurable improvements across all evaluated metrics, validating the platform's design approach.

8. Conclusion

- Integrate AI-based personalisation to recommend training based on user weaknesses.
- Add gamification and AR/VR simulations to enhance engagement and practical understanding.
- Develop a mobile application for anytime learning and improved accessibility.
- Connect with real-time threat intelligence feeds to inform users about emerging cyber attacks.
- Enable enterprise deployment and multilingual support for broader adoption across institutions and organisations.

DOI: https://dx.doi.org/10.21275/SR26311131159

The Cyber Security Awareness Platform provides an engaging way to educate users about cyber threats through learning modules, simulations, and quizzes. The system enhances user awareness, encourages safe online behaviour, and lowers human-related security risks. Its scalable design and hands-on learning features make it suitable for students, employees, and general users, with strong potential for future growth into a full cybersecurity training solution.

By integrating multimedia content, phishing simulations, gamified assessments, and performance analytics into a single unified platform, the system addresses the core gaps identified in existing cybersecurity awareness solutions. The experimental evaluation confirms significant improvements in phishing detection, quiz performance, simulation success, and overall awareness scores, demonstrating the platform's practical effectiveness.

References

[1] NIST, Cybersecurity Awareness Training Guide. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50.pdf

[2] ENISA, Cybersecurity Culture Guidelines. Available: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines

[3] SANS Institute, Security Awareness Planning Kit. Available: https://www.sans.org/security-awareness-training/resources/security-awareness-planning-kit/

[4] Kaspersky, Cybersecurity Awareness and Training Overview. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security-awareness

[5] Cisco, Cybersecurity Awareness Training Solutions. Available: https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html

[6] IBM, Cost of a Data Breach Report (Human Factor Insights). Available: https://www.ibm.com/security/data-breach

[7] Google Safety Centre, Online Security Awareness Resources. Available: https://safety.google/security/security-tips/

[8] J. Mungo, “Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks,” *Journal of Cyber Security Technology*, vol. 8, no. 2, pp. 71–119, 2023.

[9] G. A. Ali, “Protecting users from phishing email through awareness and training,” *Indian Journal of Science and Technology*, vol. 12, no. 25, pp. 1–9, 2019.

[10] M. H. Khan and S. T. Muntaha, “Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks,” *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 1663–1673, 2024.

[11] S. Kuraku, D. Kalla, N. Smith, and F. Samaah, “Exploring how user behavior shapes cybersecurity awareness in the face of phishing attacks,” *International Journal of Computer Trends and Technology*, vol. 71, no. 11, pp. 74–79, 2023.

[12] A. Alruwaili, “A review of the impact of training on cybersecurity awareness,” *International Journal of Advanced Research in Computer Science*, 2020.