IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153137

A Smart Cybersecurity Awareness Website for User Education via Courses and Gamified Learning

Rakhangi Mohammad Saif[1], Maniyar Mohammad[2], Shaikh Shahim[3], Shaikh Rehan[4], Shaikh Shahista[5]

Computer Engineering, Anjuman – I – Islam's Abdul Razzak Kalsekar Polytechnic, Navi Mumbai, India[1,2,3,4]

Lecturer, Computer Engineering, Anjuman – I – Islam's Abdul Razzak Kalsekar Polytechnic, Navi Mumbai, India[5]

Abstract: Users in today's digital environment often struggle to understand and apply cybersecurity concepts due to a lack of structured and engaging learning resources. Most existing cybersecurity awareness tools and training platforms provide either theoretical content or isolated quizzes, but they do not effectively combine structured learning, practical assessment, and user engagement in a single system. This paper proposes a web-based cybersecurity awareness platform that utilizes gamification to improve user engagement and learning outcomes. The system organizes cybersecurity topics such as phishing, malware, password security, and safe browsing practices into structured modules with multiple levels. It also includes interactive quizzes, real-time feedback, and scenario-based activities mapped to different difficulty levels. In addition, the system incorporates gamification elements such as points, badges, and leaderboards. This helps in improving user participation and allows continuous performance tracking. Overall, the design demonstrates how an integrated and interactive platform can support better cybersecurity understanding, engagement, and safe online practices.

Keywords: Cybersecurity awareness, Gamification-based learning, Web-based learning platform, Interactive quizzes, User engagement, Phishing detection, Malware awareness, Performance tracking, Scenario-based learning, Digital safety practices

I. INTRODUCTION

Users in today's digital environment often struggle to understand and apply cybersecurity concepts due to the lack of properly organized and engaging learning resources. Important information such as awareness of phishing, malware, password security, and safe online practices is often scattered across different platforms, making it difficult for users to connect concepts and apply them effectively in real-world situations.

A major limitation of current approaches is the absence of a unified system that combines structured learning, practical assessment, and user engagement in one platform. While some tools provide basic awareness content or simple quizzes, they fail to integrate learning modules, real-time interaction, and performance tracking. As a result, users find it difficult to identify important threats, analyze patterns, or improve their cybersecurity behavior effectively.

To address this problem, this paper proposes a web-based cybersecurity awareness platform that uses gamification techniques to enhance learning and engagement. The system organizes cybersecurity topics such as phishing, malware, password protection, and safe browsing into structured modules and connects them with interactive quizzes and scenario-based simulations. Learning activities are further enhanced by incorporating gamification elements such as points, badges, and leaderboards to motivate users and improve participation.

The main objective of this work is to demonstrate how a well-designed, gamified learning platform can support effective knowledge delivery, continuous assessment, and improved user awareness. The proposed system enables structured learning, real-time feedback, and performance tracking, making it suitable for applications such as cybersecurity training and awareness programs, while maintaining a strong focus on user engagement and practical learning outcomes.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026
DOI: 10.17148/IJARCCE.2026.153137

II. LITERATURE REVIEW

A. AI-Based Learning Systems

AI-based learning systems provide personalized learning experiences by analyzing user performance and behavior. These systems can recommend content, adjust difficulty levels, and improve learning efficiency. However, many existing solutions focus mainly on personalization and do not effectively incorporate cybersecurity-specific structured learning or real-time threat-based simulations, limiting their practical application in awareness training.

B. Cybersecurity Awareness Platforms

Existing cybersecurity awareness platforms provide basic educational content such as tutorials, videos, and quizzes related to threats like phishing and malware. While these platforms help in improving theoretical knowledge, they often lack interactive features and do not effectively engage users. Additionally, most systems do not integrate gamification elements, resulting in lower user motivation and participation.

C. Gamification-Based Learning Systems

Gamification-based systems enhance learning by incorporating elements such as points, badges, and leaderboards. These systems improve user engagement, motivation, and retention of knowledge. However, many gamified platforms are generic and not specifically designed for cybersecurity education. The proposed system applies gamification in a targeted manner for cybersecurity awareness, ensuring both engagement and practical learning.

D. Simulation and Scenario-Based Learning Systems

Recent systems focus on scenario-based learning and simulations to train users in identifying real-world cyber threats. These approaches are effective in improving practical understanding and decision-making skills. However, such systems are often complex and may lack integration with structured learning modules and performance tracking.

The proposed system integrates structured cybersecurity content, gamification techniques, and scenario-based assessments within a single web-based platform to provide an interactive and effective cybersecurity awareness solution.

III. SYSTEM OVERVIEW

The proposed system is a web-based cybersecurity awareness platform designed to educate users about cyber threats and promote safe online practices. The system focuses on providing an interactive, structured, and engaging learning experience using gamification techniques to improve user participation and knowledge retention.

A. System Overview

The system is built around the concept of integrating structured learning modules, interactive quizzes, gamification elements, performance tracking, and a user-friendly interface into a single platform supported by a centralized database.

B. System Components

The system is comprised of the following modules:

- Learning Module (Cybersecurity Topics)
- Quiz and Assessment Module
- Gamification Engine (Points, Badges, Leaderboards)
- Performance Tracking Module
- User Interface

C. System Workflow

The system begins with user registration and login, followed by access to structured cybersecurity learning modules. Users interact with the platform by completing lessons and participating in quizzes and scenario-based activities. The system processes user responses, provides real-time feedback, and updates scores through the gamification engine. User performance data is stored and analyzed to track progress and display results through dashboards and leaderboards, ensuring continuous engagement and learning improvement.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153137

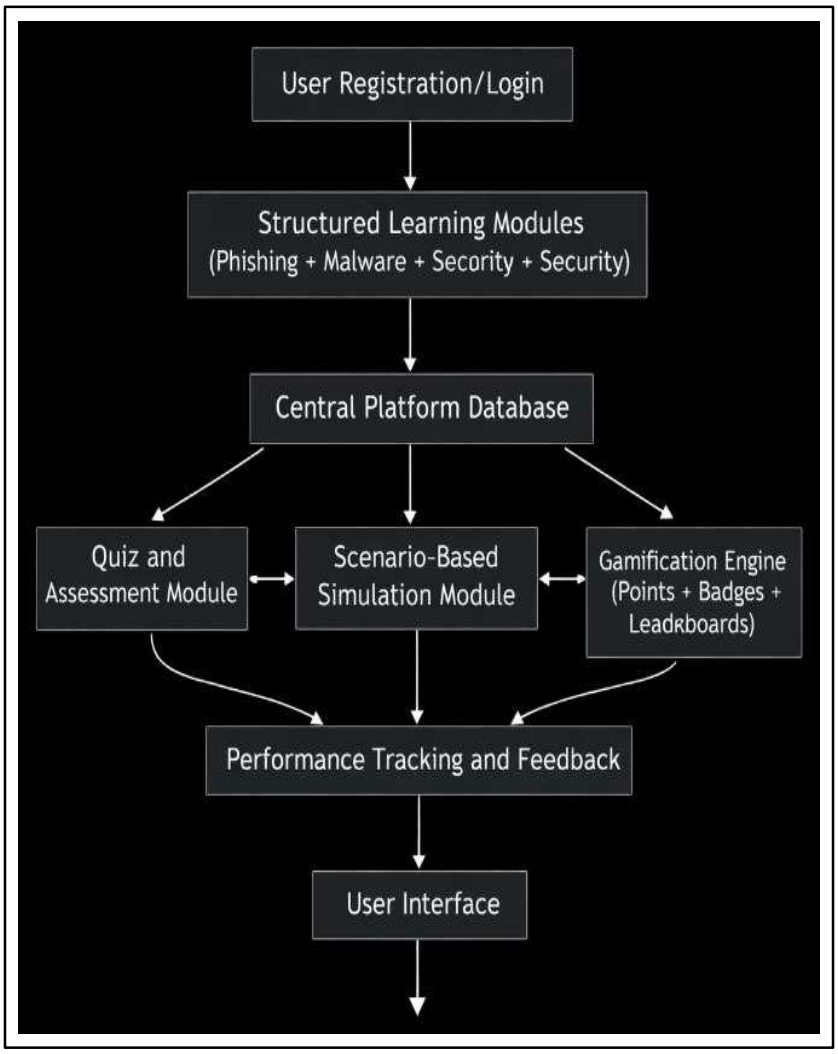

Fig. 1 Architecture of Web-Based Cybersecurity Awareness System

IV. DATABASE ARCHITECTURE

A. Database Design Goals

The database is designed to efficiently manage structured cybersecurity learning data and support intelligent operations for user engagement and assessment. The system focuses on organizing educational content, tracking user performance, and enabling gamification features. The key goals of the database include:

- Representation of structured cybersecurity learning content
- Integration of cyber threat scenarios with learning modules
- Support for quiz-based assessment and evaluation
- Gamification data management (points, badges, leaderboard)
- Scalability for multiple users and content expansion

B. Core Entity Groups

The database is logically divided into multiple entity groups to ensure modularity and efficient data handling:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153137

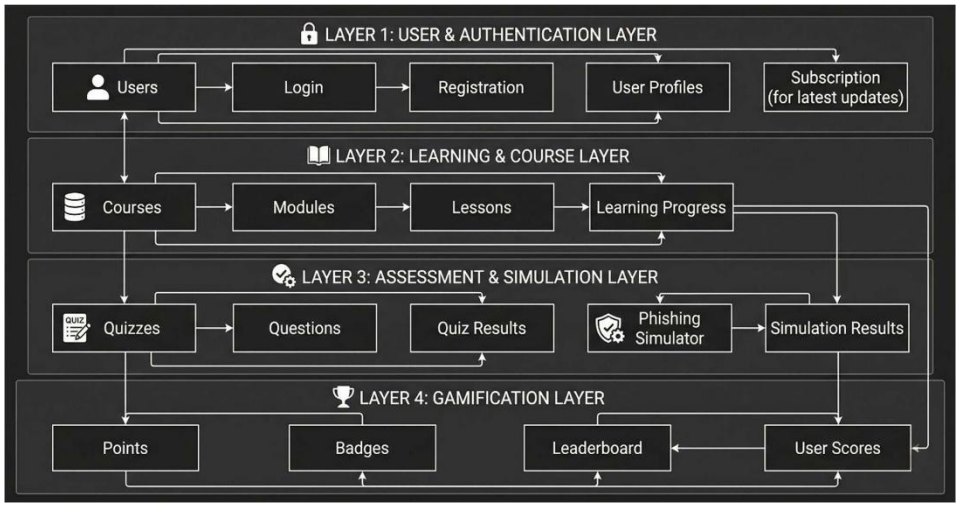

Fig. 2 Layered Database Architecture of the Proposed Cybersecurity Awareness System

1) Learning Content Layer

This layer represents the hierarchical structure of cybersecurity education. It includes modules, topics, lessons, and learning outcomes, ensuring organized and progressive content delivery.

2) Threat Intelligence Layer

This layer stores information related to cybersecurity threats such as phishing, malware, and social engineering attacks. It maps these threats to relevant learning content and supports scenario-based learning.

3) Assessment & Gamification Layer

This layer manages quizzes, questions, scores, and gamification elements. It stores user responses, calculates scores, and assigns rewards such as points, badges, and leaderboard rankings.

4) User Data Layer

This layer handles user-related information including profiles, progress tracking, performance reports, and activity logs. It enables personalized learning and continuous monitoring.

Unlike traditional systems where learning content and assessment are handled separately, the proposed database integrates content, threat intelligence, and user performance into a unified structure. This allows the database to actively support decision-making, personalized learning, and performance analysis.

C. Conceptual Data Model

The system models relationships between users, learning content, and cybersecurity assessments through an interconnected relational schema:

- Modules are divided into topics and lessons
- Cyber threats are mapped to specific lessons
- Questions are linked to topics and difficulty levels
- Users attempt quizzes and generate performance data
- Gamification elements are assigned based on performance

This integrated model enables efficient querying, personalized learning, and performance tracking.

D. Schema Design Rationale

The database follows a normalized relational structure to ensure data consistency and reduce redundancy. Mapping tables are used to handle relationships between threats, lessons, and questions. The separation of content, assessment, and user data improves modularity. Flexible fields can be used to store gamification rules and leaderboard configurations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153137

E. Key Tables and Relationships

TABLE I: CORE DATABASE TABLES AND THEIR FUNCTIONS

Table Name	Role	Purpose
users	User data	Stores user information
modules	Content	Stores cybersecurity modules
topics	Content	Defines topic-level breakdown
lessons	Content	Stores detailed learning content
threats	Threat data	Stores cyber threat information
threat_mapping	Mapping	Links threats to lessons
quizzes	Assessment	Stores quiz details
questions	Assessment	Stores quiz questions
user_scores	Performance	Stores user results
badges	Gamification	Stores reward badges
leaderboard	Ranking	Stores user rankings

F. Database Workflow

The database supports a structured workflow for cybersecurity learning:

- Learning content is organized into modules and topics
- Cyber threats are stored and mapped to lessons
- Quizzes and questions are created for assessment
- Users attempt quizzes and generate performance data
- Scores are calculated and rewards are assigned
- Progress and rankings are continuously updated

This workflow demonstrates how the database enables intelligent learning, assessment, and engagement within the cybersecurity awareness platform.

V. LEARNING AND THREAT SIMULATION PROCESSING

The proposed system enhances user learning by integrating structured content delivery, real-time assessment, and cybersecurity threat simulation. Instead of traditional question mapping, the system processes user interaction data through multiple stages to improve awareness and practical understanding of cyber threats.

Initially, users interact with structured cybersecurity courses that include topics such as phishing, malware, password security, and safe browsing practices. The system then evaluates user understanding through quizzes and real-time assessments, where responses are analyzed to determine knowledge levels and learning gaps.

To further strengthen practical knowledge, the platform incorporates a phishing simulation module that exposes users to real-world attack scenarios. User actions during these simulations are recorded and analyzed to identify behavioral patterns and vulnerabilities.

Based on quiz results and simulation performance, the system generates personalized feedback and assigns gamification rewards such as points, badges, and leaderboard rankings. This continuous processing transforms raw user interaction data into meaningful insights, enabling adaptive learning and improved cybersecurity awareness.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.153137

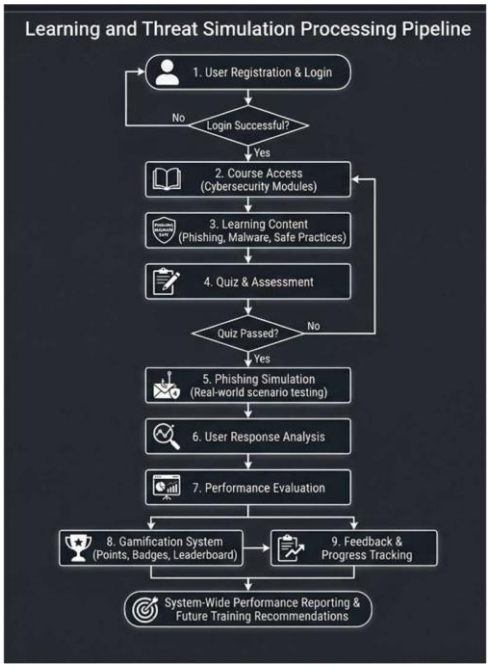

Fig. 3 Learning and Threat Simulation Processing Pipeline

VI. CONCLUSION

This research introduces a database-centric approach for managing cybersecurity learning, assessment, and user engagement. The proposed system integrates structured learning modules, threat simulation, quiz-based evaluation, and gamification features within a unified relational framework. It combines cybersecurity content, user interaction data, and performance tracking to create an effective and engaging learning environment.

The primary objective of this research is to demonstrate how the proposed architecture enables the database to go beyond traditional data storage and actively support intelligent learning, user behavior analysis, and performance-based feedback. By incorporating elements such as phishing simulation, real-time quizzes, and leaderboard-based motivation, the system enhances both theoretical understanding and practical awareness of cybersecurity threats.

Overall, the proposed system establishes a strong foundation for the development of advanced cybersecurity education platforms and interactive learning tools. It highlights the potential of integrating database design with modern educational techniques to improve awareness, engagement, and secure digital practices among users.

REFERENCES

[1]. S. Furnell and N. Clarke, "Power to the People? The Evolving Recognition of Human Aspects of Security," *Computers & Security*, vol. 31, no. 8, pp. 983–988, 2012.

[2]. M. Alotaibi, "The Role of Gamification in Enhancing Cybersecurity Awareness," *International Journal of Information Security Science*, vol. 8, no. 3, pp. 123–135, 2019.

[3]. A. T. Kabassi, I. Dragonas, and K. Ntalianis, "Evaluating a Gamified Cybersecurity Training Platform," *Journal of Information Security and Applications*, vol. 40, pp. 182–190, 2018.

[4]. S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 2007.

[5]. K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165–176, 2014.

[6]. National Institute of Standards and Technology (NIST), "Cybersecurity Framework," [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 2026].