INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 225-230
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

WEB-BASED CYBER AWARENESS SYSTEM WITH INTERACTIVE QUIZZES AND ENCRYPTION MODULES

M. Sathis kumar[1] , V. Mythri[2], A. Srividhya[3], B. Dharani[4]

[1]Professor Department of CSE (CSC) Siddhartha Institute of Technology and Science Hyderabad, India.

[2,3,4]Department of Computer Science and Engineering (CSC) Siddhartha Institute of Technology and science Hyderabad, India, 501301, India.

DOI: https://www.doi.org/10.58257/IJPREMS42764

ABSTRACT

This project presents a web-based Cyber Security Awareness platform designed to educate users about modern online threats using interactive learning modules, gamified quizzes, and practical demonstrations. As internet use grows across all age groups, so does the risk of cyberattacks targeting unaware users. This platform aims to bridge the gap between technical cybersecurity knowledge and everyday user awareness. The system allows users to learn about key topics such as phishing, malware, strong passwords, and basic cryptography through structured content and hands-on examples. Users can log in, access learning material, test their understanding with quizzes (segmented into beginner, intermediate, and advanced levels), and even simulate encryption/decryption processes. A user profile system tracks their learning journey and performance. The website is built using HTML, CSS, JavaScript, and Python with Flask, and is designed to be scalable for future integration with databases and mobile apps. This initiative contributes to promoting a cyber-aware generation that can protect themselves and others in the digital environment.

1. INTRODUCTION

The internet has become a fundamental part of modern life, enabling access to education, social networks, e-commerce, and financial systems. However, the same technologies that provide convenience also expose users to new risks. From malicious software to data breaches and scams, cyber threats are widespread and constantly evolving. According to recent studies, human error remains one of the leading causes of security incidents. This highlights the need for strong awareness and digital hygiene among all internet users.

Despite the availability of information, most people lack structured and engaging ways to learn about cybersecurity. Many resources are either too technical or unappealing, especially for students and non-technical users. As a result, awareness remains low, and users continue to fall for preventable attacks.

This project aims to solve this issue by creating a cybersecurity awareness website that is both informative and interactive. It simplifies complex topics, presents them in a visually engaging format, and encourages learning through quizzes and demonstrations. By doing so, it empowers users to recognize threats and adopt safer online habits.

Problem Statement

Many people, especially students and firsttime internet users, are unaware of basic cybersecurity concepts such as phishing, malware, and password management. The few platforms that do offer learning materials often fail to capture attention or encourage consistent learning. Most users do not understand the risks of clicking on unknown links, reusing weak passwords, or sharing sensitive data online.

Moreover, many existing tools and websites do not allow users to track their learning progress or practice concepts like encryption in a hands-on manner. This results in knowledge gaps that cybercriminals can exploit. Thus, there is a pressing need for an accessible, engaging, and easy-to-use cybersecurity learning platform that encourages self-paced learning and awareness-building through interactive features.

2. LITERATURE SURVEY

Several existing platforms and studies highlight the growing importance of cybersecurity awareness. Google’s “Be Internet Awesome” and NCA’s “StaySafeOnline” provide content tailored mostly for young audiences or businesses, respectively. These resources are helpful but often lack interactivity and regular engagement features.

Academic literature published in IEEE, ACM, and other peer-reviewed journals confirms that active learning—especially gamified and hands-on—significantly increases knowledge retention. A study titled "Gamification in Cybersecurity Education" (IEEE 2021) noted that learners using interactive platforms showed 60% higher retention than those using static content. Additionally, "CyberAware" by the UK Government has shown that national-scale awareness campaigns can drive behavioral change when paired with good design.

This project leverages such findings to build an all-in-one solution that combines structured content, hands-on activities, and self-assessment features in a single, beginnerfriendly web application.

3. CHALLENGES ADRESSED BY THE PROJECT

Lack of Awareness:

Many individuals, especially non-technical users, are unaware of common cyber threats and do not follow basic online safety practices. The project addresses this by simplifying cybersecurity concepts and making them approachable.

Limited Engagement:

Traditional awareness tools are often text-heavy and lack interaction, leading to low user interest. This platform incorporates interactive quizzes, gamified learning, and simulations to sustain user engagement.

No Feedback or Tracking:

Existing systems typically don't provide users with any insight into their learning progress. This project introduces a dashboard with scores and topic-wise feedback to help users identify strengths and areas needing revision.

4. EXISTING SYSTEM

The current landscape of cybersecurity awareness solutions can be broadly divided into:

- **Government Info Pages:** Offer reliable information but are static and lack interactivity.
- **MOOCs and Online Courses:** Although educational, these are often lengthy, complex, and not tailored for beginners.
- **Workshops and Seminars:** Effective but occur infrequently and may not reach a wide audience.
- **Posters and Campaigns:** Useful for reminders but insufficient for in-depth knowledge or behavioral change.

Overall, these systems do not offer personalized learning, real-time feedback, or ongoing engagement, which limits their effectiveness in promoting long-term cybersecurity awareness.

5. PROPOSED SYSTEM

The proposed solution is an interactive, web-based platform designed to educate users about cybersecurity in a practical and engaging way. The system consists of the following modules:

- **Awareness Pages:** Well-structured, topic-wise information on phishing, malware, password hygiene, network security, and more.
- **Quizzes:** Categorized into beginner, intermediate, and advanced levels to test understanding.
- **Encryption Simulator:** A hands-on tool to demonstrate encryption/decryption concepts.
- **User Profiles:** Allow users to log in, save their scores, and track learning progress.
- **Responsive UI:** Designed to work on mobile, tablet, and desktop platforms.
- **Admin Panel:** For managing content, users, and quiz data.

By combining educational content with interactivity, the system aims to make cybersecurity learning engaging, effective, and self-paced.

6. IMPLEMENTATION

Frontend Technologies:

- HTML5, CSS3, JavaScript
- Responsive design with simple navigation
- Dynamic quiz rendering and topic navigation

Backend Technologies:

- Python Flask for server-side logic and routing
- Local storage simulation for user session tracking (future upgrade: database integration)
- Quiz score computation and content handling

Testing:

- Functionality tested across browsers
- Mobile responsiveness verified
- Encryption input/output accuracy confirmed

Vol. 05, Issue 07, July 2025, pp : 225-230
e-ISSN : 2583-1062
Impact Factor : 7.001

Software Requirements

- **Operating System:** Windows, Linux, or macOS
- **Languages Used:** HTML, CSS, JavaScript, Python (Flask)
- **Database:** SQLite or MySQL (for future implementation)
- **Libraries& Tools:** Flask, Pyttsx3,

SpeechRecognition, TensorFlow (optional)

IDE: Visual Studio Code, Jupyter Notebook

Hardware Requirements

Client Machine:

- Dual-core processor (1.5 GHz or higher)
- 4 GB RAM
- Modern web browser (Chrome, Firefox, Edge, Safari)
- Stable internet connection •

Server Machine (for deployment):

- Quad-core processor (2 GHz or higher)
- Minimum 100 GB storage
- Static IP and hosting support

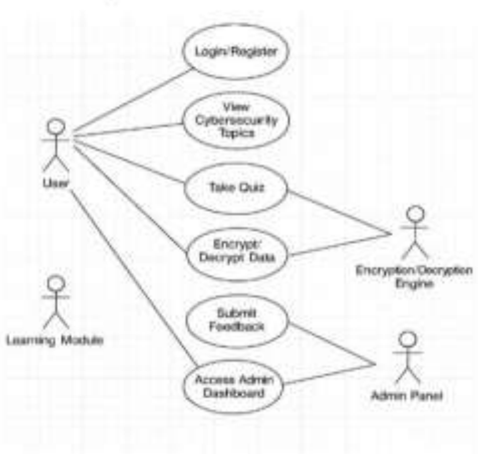
Optional Accessories:

- Microphone and speakers for voice interaction

UML DIAGRAMS

Use case diagram

This use case diagram visually represents the interaction between a user and the Cyber Security Awareness Website. It highlights the various functionalities the system offers, such as user login, accessing learning materials, attempting topic-wise quizzes, trying encryption/decryption demos, and viewing their profile progress. It helps in understanding what features are accessible to users and how each module is connected.



Class diagram

This class diagram visually illustrates the major classes and their relationships in the CyberAware system. Key components include the User, Quiz, LearningModule, EncryptionTool, and UserProfile classes. Each class handles a specific responsibility, such as storing user data, rendering quizzes, showing topics, or tracking progress. The relationships between classes show how data is passed and processed within the system.

Sequence Diagram

The sequence diagram shows the step-by-step interaction between the user and the website during a quiz attempt. It outlines the flow from selecting a topic, loading questions, submitting answers, and updating the user profile with the result. This helps demonstrate how user input is handled dynamically and stored appropriately.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 225-230
e-ISSN : 2583-1062
Impact Factor : 7.001

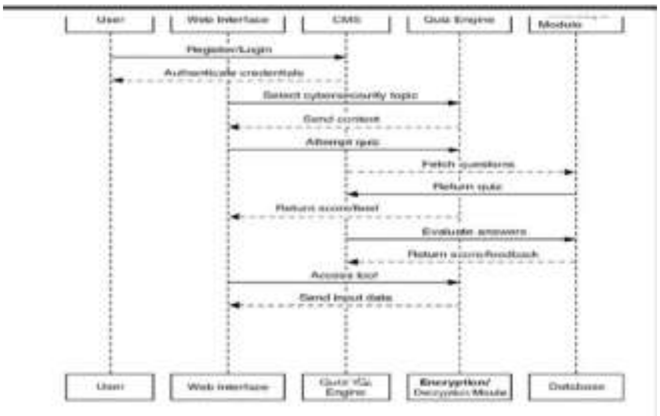


Fig 6.2.3 Sequence Diagra

This class diagram visually illustrates the major classes and their relationships in the CyberAware system. Key components include the User, Quiz, LearningModule, EncryptionTool, and UserProfile classes. Each class handles a specific responsibility, such as storing user data, rendering quizzes, showing topics, or tracking progress. The relationships between classes show how data is passed and processed within the system.

7. RESULTS

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 225-230

e-ISSN : 2583-1062
Impact Factor : 7.001

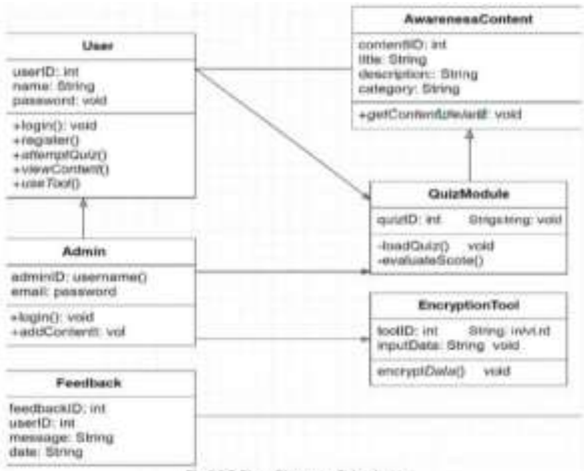


Fig 6.2.3 Class Diagram – CyberAware

8. CONCLUSION

The CyberAware website successfully bridges the gap between complex cybersecurity concepts and the general user's understanding through a well-organized, interactive learning platform. It provides educational modules, quizzes categorized by difficulty, hands-on encryption and decryption demos, and user progress tracking via profiles. The project showcases how awareness, when delivered in a visually engaging and interactive format, can significantly improve user understanding and retention of cybersecurity principles.

This platform not only raises awareness but also encourages users to adopt safe digital habits through practical exercises and evaluations. The implementation of the system using basic web technologies makes it accessible and scalable, especially for students and educational institutions aiming to promote digital safety. Through this initiative, users are empowered with the essential knowledge to recognize, prevent, and respond to cyber threats in their day-today internet usage.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 225-230
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

9. FUTURE SCOPE

- **Integration with Backend Databases**: In future, the platform can be extended to store user progress and quiz results persistently using a database like MySQL or MongoDB.
- **Admin Panel for Content Management**: Future versions could include an admin dashboard to add/edit learning content, quiz questions, or manage user roles.
- **Gamification and Leaderboards**: Adding rewards, badges, and rankings can motivate users to learn more and increase platform engagement.
- **Mobile App Version**: A dedicated mobile application could be developed for broader accessibility.
- **Multilingual Support**: Expanding the platform's content in regional languages to reach a more diverse audience across different geographies.
- **Real-time Threat Alerts and News**: Integration of live cybersecurity news or alert systems to make the portal dynamic and up-to-date.

10. REFERENCES

[1] National Cyber Security Alliance
[2] StaySafeOnline.org
[3] Google's "Be Internet Awesome"
[4] IEEE Research Paper: Gamification in Cybersecurity Education – IEEE Explore, 2021
[5] CyberAware UK Government Campaign – https://www.cyberaware.gov.uk
[6] OWASP Foundation – https://owasp.org
[7] Computer Security: Principles and Practice by William Stallings – Pearson Education
[8] TutorialsPoint: Cyber Security Basics – https://www.tutorialspoint.com/cyber_securit y
[9] MDN Web Docs for HTML, CSS, and JavaScript – https://developer.mozilla.org