CYBERAEGIZ: COMPREHENSIVE CYBERSECURITY SUITE

Wan Aiman Bin Wan Ibrahim
Kulliyyah of Information and Communication Technology
Department of Computer Science
International Islamic University Malaysia
wanaimanwanibrahim@gmail.com

Ahmad Nazrin Bin Ahmad Khalil
Kulliyyah of Information and Communication Technology
Department of Computer Science
International Islamic University Malaysia
nazrin.izwan@iium.edu.my

Dr. Adamu Abubakar Ibrahim
Kulliyyah of Information and Communication Technology
Department of Computer Science
International Islamic University Malaysia
adamu@iium.edu.my

Abstract—**This paper presents CyberAegiz, a unified platform designed to address modern cybersecurity challenges by integrating phishing detection, password management, encryption and decryption services, and an education hub. Developed using the MERN stack, the platform combines MongoDB for efficient data management, Express.js and Node.js for scalable backend services, and React.js for a dynamic user interface. CyberAegiz is informed by a comparative analysis of existing systems, addressing gaps such as user education and accessibility while simplifying essential cybersecurity tools. Testing and evaluation demonstrate the platform's effectiveness in providing user-friendly solutions for individuals and SMEs. While certain constraints, such as limited scalability and incomplete educational content, remain, future work will include the integration of machine learning for adaptive phishing detection, expansion of educational resources, and development of a mobile application. CyberAegiz establishes a scalable and user-centric foundation for improving cybersecurity awareness and protection.**

Keywords—Cybersecurity, phishing detection, password management, encryption, education hub.

I. INTRODUCTION

This section provides an overview of the project by describing the chosen organisation and providing background information that is related to the project.

A. Background

Cyberattacks are becoming more sophisticated and common as the digital world grows. Hence, leaving many individuals and businesses vulnerable to various new or existing threats. Password management, phishing detection and data encryption are just a few examples of the specialized services offered by traditional cybersecurity solutions. While these apps may contain the necessary security features, they usually work in isolation and cannot provide a comprehensive defense system against the many online threats. Furthermore, traditional instruments often use detection approaches based on static signatures. This are not very good at preventing complex and ever-changing intrusions or zero-day vulnerabilities. In proposing a unified, user-friendly platform that incorporates a suite of advanced security tools, CyberAegiz represents a paradigm shift in the approach to cybersecurity. Not only does this comprehensive strategy seek to safeguard against cyber hazards, but it also seeks to inform users on how to maintain a secure online presence. Nevertheless, the development of a solution that effectively balances user accessibility with advanced security measures will present a distinctive set of challenges. These challenges would include the integration of a variety of security functionalities. Plus, the adaptation to new and emerging threats and the necessity of fostering user trust and comprehension of cybersecurity principles would also be included.

B. Problem Description

In an increasingly digital environment, a wide range of sophisticated cyber attacks is widespread and conventional cybersecurity solutions are unable to keep up with the fast advancement of these threats. The existing solutions would often function independently and target individual risks without a cohesive strategy to offer all-encompassing safeguarding. The current state of security is divided and disorganized. It will leave all the consumers vulnerable to advanced attacks like phishing, malware and zero-day exploits. Therefore, it is very essential to adopt additional dynamic and integrated defense systems. CyberAegiz presents a suitable approach by suggesting a scalable comprehensive cybersecurity platform that combines modern technologies like real time phishing detection extension with necessary cybersecurity security tools. Moreover, this technique not only fills the holes caused by outdated methods but also improves the system's capacity to quickly adjust to new emergent threats. CyberAegiz strives to provide comprehensive and user-friendly cybersecurity services that enable clients with varying levels of technical knowledge to effectively safeguard their online presence. This solution is designed to have both resilience and usability in order to effectively respond to the constantly changing digital risk environment.

C. Project Objective

The primary objective of this project is to design and develop a unified cybersecurity platform that integrates essential web and data security tools into a cohesive system. This platform aims to include critical functionalities such as phishing detection, password strength analysis, encryption and decryption services, and a password generator.

Alongside these features, the platform incorporates an educational component designed to enhance users' understanding of cybersecurity practices and promote better digital security habits. Additionally, the team seeks to develop a functional prototype of the platform and rigorously test and validate its performance to ensure it meets user requirements and effectively addresses evolving cybersecurity challenges*Project Objective*

The primary objective of this project is to design and develop a unified cybersecurity platform that integrates essential web and data security tools into a cohesive system. This platform aims to include critical functionalities such as phishing detection, password strength analysis, encryption and decryption services, and a password generator. Alongside these features, the platform incorporates an educational component designed to enhance users' understanding of cybersecurity practices and promote better digital security habits. Additionally, the team seeks to develop a functional prototype of the platform and rigorously test and validate its performance to ensure it meets user requirements and effectively addresses evolving cybersecurity challenges

D. Project Scope

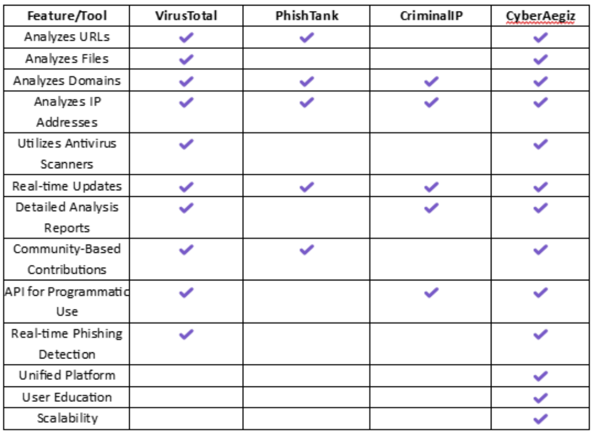
The objective of this project was to deliver a unified cybersecurity platform. The programme aims to be user-friendly which cater to users with varying levels of technical expertise and enabling them to simply and effectively protect their digital information from a broad spectrum of cyber threats. In order to evaluate the prototype's performance and user experience. This project will conduct surveys and usability testing with potential end users. The purpose of these evaluations is to collect feedback on the application's interface, functionality and overall usability, in order to make necessary adjustments and improvements. In addition, the CyberAegiz application will employ scalable and adaptive technologies, such as real time phishing detection extension to ensure that its security measures advance with developing cyber threats. Therefore it will surely create a more robust defense mechanism. The primary objective of CyberAegiz is to provide a user-friendly and readily available platform that empowers not only IT professionals, but also individuals and SMEs, to effectively uphold a secure online existence. The team aims to fill the existing deficiencies in current cybersecurity methods by offering a comprehensive solution that enhances the understanding and implementation of digital security throughout its user community.

II. Literature Review

A. Existing Systems

The study of existing systems provides insights into the strengths and limitations of current tools in the field of cybersecurity. This analysis informs the design of CyberAegiz, ensuring that it incorporates essential features while addressing gaps in the market. A comparative evaluation of tools for phishing detection, password management, and encryption and decryption was conducted.

I. Phishing Detection Tools

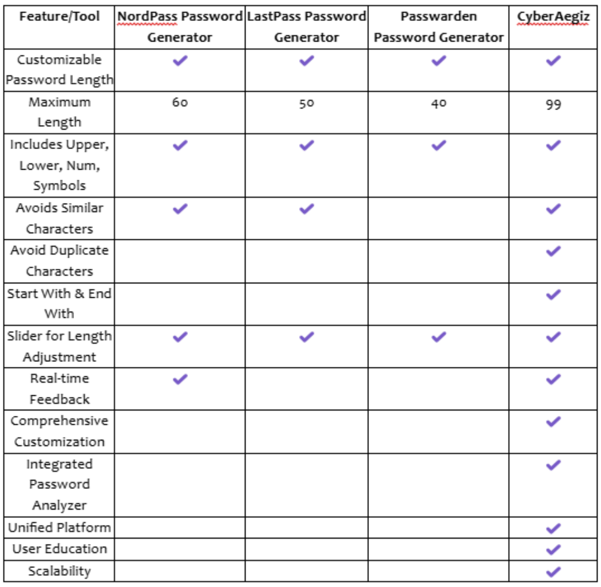


Feature/Tool	VirusTotal	PhishTank	CriminalIP	CyberAegiz
Analyzes URLs	✓	✓		✓
Analyzes Files	✓			✓
Analyzes Domains	✓	✓	✓	✓
Analyzes IP Addresses	✓	✓	✓	✓
Utilizes Antivirus Scanners	✓			✓
Real-time Updates	✓	✓	✓	✓
Detailed Analysis Reports	✓		✓	✓
Community-Based Contributions	✓	✓		✓
API for Programmatic Use	✓		✓	✓
Real-time Phishing Detection	✓			✓
Unified Platform				✓
User Education				✓
Scalability				✓

TABLE I. PHISHING DETECTION TOOLS COMPARISON BETWEEN EXISTING SYSTEMS

Acomparison of phishing detection tools such as VirusTotal, PhishTank, and CriminalIP reveals variations in feature sets. These tools analyze URLs, files, domains, and IP addresses, with some offering detailed analysis reports and real-time updates. However, CyberAegiz simplifies these features for ease of use while excluding real-time phishing detection, focusing instead on static analysis methods to evaluate links and files for potential threats.

II. Password Management Tools

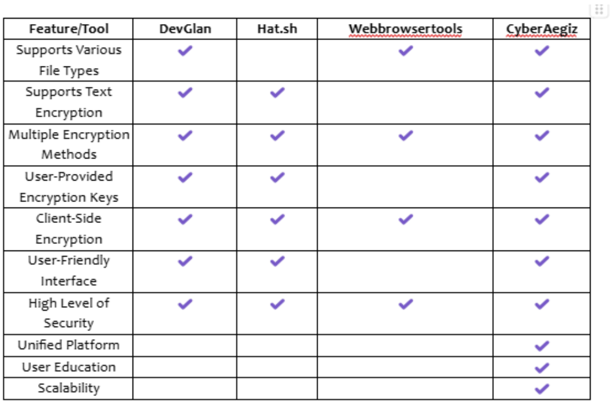


Feature/Tool	NordPass Password Generator	LastPass Password Generator	Passwarden Password Generator	CyberAegiz
Customizable Password Length	✓	✓	✓	✓
Maximum Length	60	50	40	99
Includes Upper, Lower, Num, Symbols	✓	✓	✓	✓
Avoids Similar Characters	✓	✓		✓
Avoid Duplicate Characters				✓
Start With & End With				✓
Slider for Length Adjustment	✓	✓	✓	✓
Real-time Feedback	✓			✓
Comprehensive Customization				✓
Integrated Password Analyzer				✓
Unified Platform				✓
User Education				✓
Scalability				✓

TABLE II. PASSWORD MANAGEMENT TOOLS COMPARISON BETWEEN EXISTING SYSTEMS

Password management tools, including NordPass, LastPass, and Passworden, were evaluated for their capabilities in generating and analyzing passwords. These tools typically allow customization of password length and complexity, including features to avoid similar or duplicate characters. CyberAegiz extends these functionalities with higher maximum password lengths, comprehensive customization options, and integrated password strength analysis, providing users with actionable feedback on password security.

III. Encryption and Decryption Tools



Feature/Tool	DevGlan	Hat.sh	Webbrowsertools	CyberAegiz
Supports Various File Types	✓		✓	✓
Supports Text Encryption	✓	✓		✓
Multiple Encryption Methods	✓	✓	✓	✓
User-Provided Encryption Keys	✓	✓		✓
Client-Side Encryption	✓	✓	✓	✓
User-Friendly Interface	✓	✓		✓
High Level of Security	✓	✓	✓	✓
Unified Platform				✓
User Education				✓
Scalability				✓

TABLE III. ENCRYPTION & DECRYPTION TOOLS COMPARISON BETWEEN EXISTING SYSTEMS

Encryption and decryption tools such as DevGlan, Hat.sh, and Webbrowsertools were studied for their support of file types, encryption methods, and client-side processing. While these tools focus on secure data handling, CyberAegiz adds value by incorporating a unified platform for file encryption and decryption along with basic educational content on secure data practices.

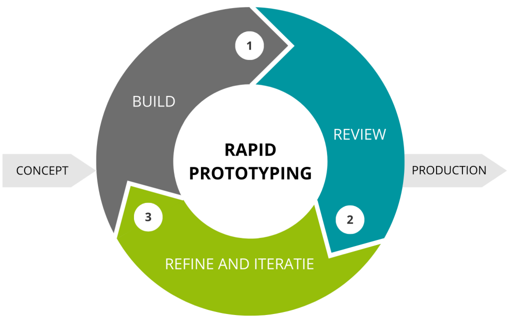
B. Summary of System Adaptation

The design of CyberAegiz draws from the strengths of existing systems while addressing their limitations. For example, while most phishing detection tools require technical expertise to interpret results, CyberAegiz provides user-friendly outputs that cater to a broader audience. Similarly, its password management and encryption tools integrate functionality and ease of use, with customization options designed for both novice and advanced users.

The comparative evaluation in this chapter demonstrates the need for a unified platform that simplifies access to essential cybersecurity tools while promoting user education. CyberAegiz addresses this need, serving as an accessible and comprehensive solution for cybersecurity challenges.

III. Methodology

A. Development Approach



Rapid prototyping is a software development approach that tests product functionality, designs and usability. This could be done by quickly creating and revising prototypes. Projects that require regular feedback and adaptation benefit from this method. Since developers can quickly discover and fix design problems and user requirements. Rapid prototyping lets developers quickly reach a design by prototyping, testing and also refining.

Rapid prototyping is essential for CyberAegiz's comprehensive cybersecurity web application with superior security features. The ability to rapidly prototype helps the development team to test and improve security features. This will include phishing detection, password strength analysis and encryption due to cyber threats' complexity. Continuous user input supports this iterative approach. This will ensure the final product satisfies target audience security and usability criteria.

CyberAegiz chose fast prototyping for numerous compelling reasons:

Feedback-oriented development: Cybersecurity solutions must be user-friendly and effective against real-world threats. Rapid prototyping allows for constant testing and feedback. This could improve the application's security and user experience.

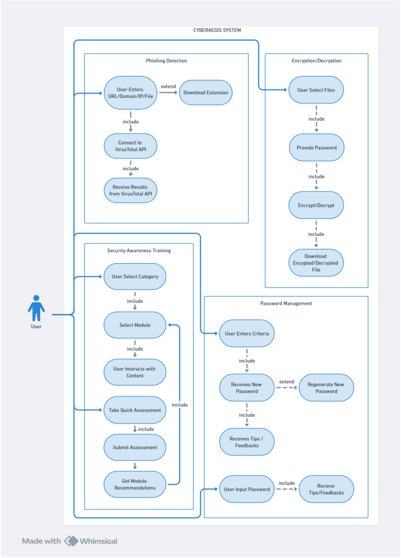
Flexibility: Cyber dangers change, therefore security technologies must have timely updates. Rapid development lets the project absorb new technologies and threat data. It will keep the app updated and effective.

Cost-Efficiency: Effective resource management is crucial for student-led projects. Rapid prototyping reduces project costs by discovering difficulties early in development eliminating the need for rework.

Educational Value: Rapid prototyping gives team members expertise in iterative development, testing and user feedback analysis for educational programs like CyberAegiz which emphasize learning and adaptability.

Finally, rapid prototyping is suitable for CyberAegiz's objective of establishing a flexible, user-centered and adaptable cybersecurity platform. This technique helps the project's technical progress and gives developers real experience in current software development.

B. Use Case Diagram



I. Phishing Detection Tool

The phishing detection tool allows the **user** to input a URL, domain, IP address, or file for analysis. The system sends the input to the VirusTotal API and displays the results (e.g., Safe, Suspicious, Malicious). If the input is invalid, the system prompts the user to provide valid data. Users can also download a browser extension for real-time detection. The tool ensures users are informed about the safety of their submissions.

II. Password Management Tool

The password management tool enables users to generate secure passwords based on specified criteria (e.g., length, symbols) and provides real-time feedback on password strength. Users can also validate existing passwords. If the password is weak, users can regenerate or adjust it. The system ensures users receive secure, client-generated passwords or feedback on their current credentials.

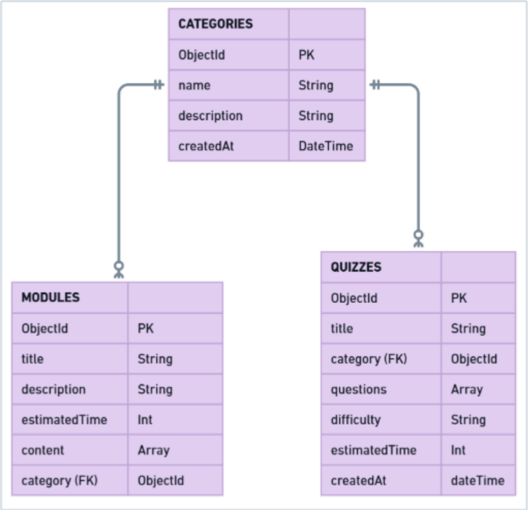
III. Encryption and Decryption Tool

The encryption and decryption tool allows users to upload files for encryption or decryption using a password. The system processes the file locally and enables secure downloading. If an incorrect password is entered, the system prompts for reentry. This ensures that files are securely encrypted or decrypted as requested.

IV. Security Awareness Training

The security awareness training module provides educational content, including reading materials, videos, and quizzes. Users can select categories or take a quick assessment, which evaluates their knowledge and recommends relevant modules. The system ensures personalized learning by guiding users to appropriate content based on their assessment results.

C. Entity Relationship Diagram



CATEGORIES	
ObjectId	PK
name	String
description	String
createdAt	DateTime

MODULES	
ObjectId	PK
title	String
description	String
estimatedTime	Int
content	Array
category (FK)	ObjectId

QUIZZES	
ObjectId	PK
title	String
category (FK)	ObjectId
questions	Array
difficulty	String
estimatedTime	Int
createdAt	dateTime

The **Entity-Relationship (ER) Diagram** for the CyberAegiz platform illustrates the database structure designed to support the educational features of the system, particularly the **Education Hub**. This diagram consists of three main entities: **Categories**, **Modules**, and **Quizzes**, with defined relationships to ensure data organization and integrity.

The database design for the CyberAegiz Education Hub offers several key benefits that enhance its scalability, integrity, and user-centric functionality. The structure is designed to be highly scalable, allowing new categories, modules, and quizzes to be seamlessly added without impacting the existing data. Strong relationships between entities ensure data integrity, as all modules and quizzes are linked to valid categories, maintaining consistency across the system. Additionally, the design focuses on user experience by supporting efficient content retrieval, enabling users to easily navigate and access relevant educational resources and assessments. The inclusion of arrays for content and questions adds flexibility, allowing the storage of diverse data types such as text, multimedia, and links, which enriches the user learning experience. This thoughtful design ensures the platform is robust, adaptable, and capable of meeting the evolving needs of its users.

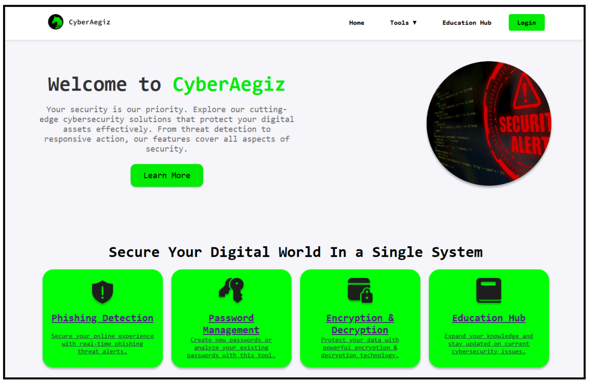
IV. RESULTS

A. System Overview

The CyberAegiz platform provides an integrated solution for digital security through its four main features: phishing detection, password management, encryption and decryption, and the education hub. Each feature is designed with usability and functionality in mind, leveraging the MERN stack for responsive and scalable performance.

B. System Pages and Functionalities

I. Home Page



Welcome to CyberAegiz

Your security is our priority. Explore our cutting-edge cybersecurity solutions that protect your digital assets effectively. From threat detection to responsive action, our features cover all aspects of security.

Secure Your Digital World In a Single System

Phishing Detection: Secure your online experience with real-time phishing threat alerts.

Password Management: Create new passwords or analyze your existing passwords with this tool.

Encryption & Decryption: Protect your data with powerful encryption & decryption technology.

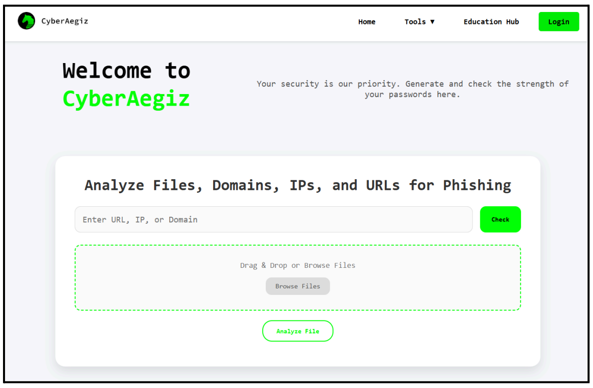
Education Hub: Expand your knowledge and stay updated on current cybersecurity issues.

Description: The **home page** welcomes users with an overview of CyberAegiz's features and functionalities. It emphasizes user security and provides quick navigation to different tools.

The homepage serves as the main entry point for users, providing an overview of the platform and quick access to key features like phishing detection, password management, encryption and decryption, and the education hub. Test cases validated the following functionalities:

- **Navigation**: Links to different sections of the platform, including Tools and Education Hub, were tested to ensure seamless navigation.
- **Dynamic Display**: The homepage dynamically displays core information and encourages user engagement with a clean and responsive design.
- **Responsiveness**: The page was tested across multiple devices and screen resolutions to confirm its compatibility and adaptability. All test cases passed, confirming the homepage’s ability to guide users effectively and enhance their overall experience.

II. Phishing Detection Tool



Welcome to CyberAegiz

Your security is our priority. Generate and check the strength of your passwords here.

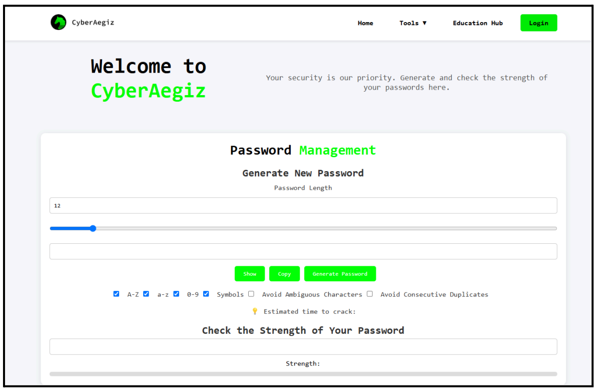
Analyze Files, Domains, IPs, and URLs for Phishing

Enter URL, IP, or Domain

Description: The **phishing detection tool** is a dedicated page where users can analyze files, domains, IP addresses, and URLs for potential phishing threats. The tool offers options for entering URLs or domains manually and supports file analysis through drag-and-drop or file upload functionality. Upon submission, the system processes the input and dynamically displays results, ensuring an interactive and seamless experience.

The phishing detection tool was tested to ensure it accurately processes user inputs, including URLs, domains, IP addresses, and files, to detect potential phishing threats. Test cases validated functionalities such as input validation, API requests for phishing analysis, and dynamic result display. All scenarios, including edge cases like invalid or empty inputs, performed as expected, ensuring reliability and user satisfaction.

III. Password Management Tool



Welcome to CyberAegiz

Your security is our priority. Generate and check the strength of your passwords here.

Password Management

Generate New Password

Password Length

12

☑ A-Z ☑ a-z ☑ 0-9 ☑ Symbols □ Avoid Ambiguous Characters □ Avoid Consecutive Duplicates

💡 Estimated time to crack:

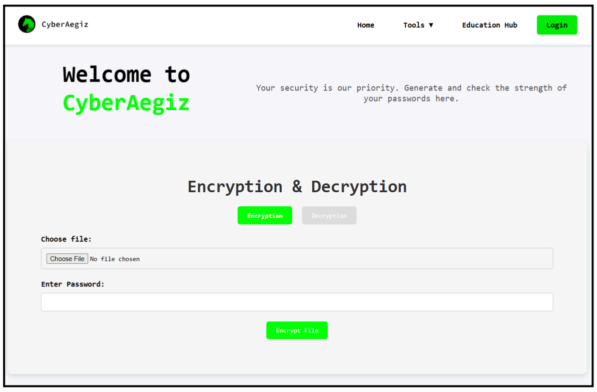
Check the Strength of Your Password

Strength:

Description: The **password management tool** focuses on helping users generate secure passwords and analyze the strength of existing ones. It allows users to customize the length and complexity of passwords by adjusting sliders and toggling character options. The system also provides feedback on the estimated time to crack a password, empowering users to make informed decisions about their security.

The password management tool underwent extensive testing for functionalities such as password generation, customization, copying, and strength evaluation. Features like adjusting password length, avoiding duplicate characters, and checking password strength were tested thoroughly. Each test case passed, confirming the tool's ability to create secure passwords and provide real-time feedback effectively.

IV. Encryption and Decryption Tool



Welcome to CyberAegiz

Your security is our priority. Generate and check the strength of your passwords here.

Encryption & Decryption

Choose file:

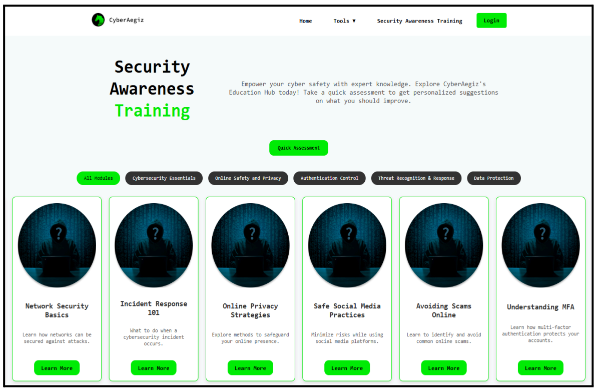
Choose File No file chosen

Enter Password:

Description: The **encryption and decryption tool** enables users to secure their data through file encryption and decryption. Users can upload files and apply a custom password for encryption. The tool supports decryption of previously encrypted files, ensuring data security throughout the process. The page offers straightforward functionality for these critical tasks, making it accessible to both technical and non-technical users.

This tool was evaluated for its ability to encrypt and decrypt files using user-defined passwords. Test cases verified the accuracy of file encryption and decryption processes, handling of invalid inputs, and file download functionality. The tool demonstrated robustness in securing user data, with all test cases yielding expected results.

V. Education Hub



Security Awareness Training

Empower your cyber safety with expert knowledge. Explore CyberAegiz's Education Hub today! Take a quick assessment to get personalized suggestions on what you should improve.

Network Security Basics

Learn how networks can be secured against attacks.

Incident Response 101

What to do when a cybersecurity incident occurs.

Online Privacy Strategies

Explore methods to safeguard your online presence.

Safe Social Media Practices

Minimize risks while using social media platforms.

Avoiding Scams Online

Learn to identify and avoid common online scams.

Understanding MFA

Learn how multi-factor authentication protects your accounts.

Description: The **education hub** serves as a resource center for cybersecurity knowledge and awareness. It includes a quick assessment feature that allows users to test their understanding of cybersecurity concepts. The hub is designed to provide educational modules on topics such as phishing, password security, and data encryption. However, some areas of the hub, such as module content, are currently placeholders, indicating opportunities for future expansion.

The education hub was tested for navigation, content display, and the functionality of the quick assessment feature. Although the hub includes placeholder content for future expansion, existing functionalities, such as presenting educational resources and conducting assessments, were verified to operate seamlessly.

V. CONCLUSION

A. Completed Requirements

The project successfully delivered on its core functionalities, ensuring that users can interact with a reliable and user-friendly interface. Key features, such as the phishing detection tool, password management system, and encryption services, were implemented and tested to meet specified requirements. The education hub, while functional, provides a foundation for further enhancements with plans to include more comprehensive modules and resources. These achievements underscore the viability of CyberAegiz as a platform that empowers users to protect their digital assets effectively.

B. *Uncompleted Requirements*

Despite the success of the project, certain planned components were either partially implemented or left incomplete due to constraints. The educational modules within the education hub remain underdeveloped, with placeholder content awaiting expansion. Additionally, advanced functionalities such as detailed phishing analysis reports and multi-language support were identified as areas for future improvement but were not implemented within the current project scope.

C. *Project Constraints*

The project faced several constraints that impacted its development and implementation. Time limitations restricted the inclusion of advanced features and extensive testing for scalability. Resource constraints also influenced the depth of content in the education hub and the sophistication of certain tools, such as real-time phishing detection. Furthermore, the absence of a dedicated mobile application limited the platform's accessibility for on-the-go users, highlighting an opportunity for further growth.

D. *Future Enhancements*

Expansion of Educational Modules
Comprehensive educational resources are essential to foster cybersecurity awareness. Adding interactive content, such as step-by-step tutorials, videos, and gamified quizzes, will enhance the learning experience and encourage active user participation.

Integration of Machine Learning
Real-time threat analysis can be significantly improved by incorporating machine learning. Adaptive algorithms would allow the phishing detection tool to identify emerging threats dynamically, ensuring robust protection against evolving cyberattacks.

Mobile Application Development
Developing a mobile version of CyberAegiz will increase accessibility, enabling users to secure their digital presence conveniently from any device. A mobile app will support on-the-go use and provide instant notifications for detected threats.

Scalability Optimization
To prepare for larger user bases, optimizing the system architecture for scalability is vital. Migrating to a cloud-based infrastructure will ensure seamless performance under high traffic conditions, making CyberAegiz suitable for enterprise-level use.

Multi-Language Support
Introducing multi-language options will broaden the platform's reach, making it accessible to non-English speakers and fostering inclusivity. This addition would cater to diverse users and promote cybersecurity awareness globally.

Finally, these enhancements align with CyberAegiz's mission to provide a flexible, user-centered, and innovative platform. By addressing these areas, the system will continue to evolve as a leading solution in digital security.

REFERENCES

[1] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, pp. 13–21, 2014.

[2] M. Bay, "What is cybersecurity? In search of an encompassing definition for the post-Snowden era," *French Journal for Media Research*, no. 6, 2016. [Online]. Available: https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era

[3] P. Sharma and K. Saharan, "Visual similarity-based phishing detection techniques for web security," *Security and Communication Networks*, 2017. [Online]. Available: https://doi.org/10.1155/2017/5421046

[4] R. Goyal and M. Khurana, "Cryptographic security using various encryption and decryption methods," *I.J. Mathematical Sciences and Computing*, vol. 3, pp. 1–11, 2017.

[5] Springer, *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing,* vol. 169, Studies in Systems, Decision and Control, Springer, Cham, 2020. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-40417-8_8

[6] B. M. Nema and H. A. AL Wally, "Cybersecurity risks detection and prevention," *Al-Mansour Journal*, 2019. [Online]. Available: https://www.iasj.net/iasj/download/b49104f5f1070b70

[7] Sarker *et al.*, "Cybersecurity data science: An overview from a machine learning perspective," *Journal of Big Data*, vol. 7, art. no. 73, 2020. [Online]. Available: https://link.springer.com/article/10.1186/s40537-020-00318-5

[8] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014. [Online]. Available: https://doi.org/10.1016/j.jcss.2014.02.005

[9] Martínez Torres *et al.*, "Machine learning techniques applied to cybersecurity," *International Journal of Intelligent Systems*, vol. 34, no. 10, pp. 2317–2338, 2019. [Online]. Available: https://doi.org/10.1002/int.22174

[10] D. Goyal, G. Lavania, and G. Sharma, "Review of modern web application cybersecurity risks and counter measures," *AIP Conference Proceedings*, vol. 2782, no. 1, art. no. 020204, 2023. [Online]. Available: https://doi.org/10.1063/5.0047605

[11] Y. Ma and N. W. Twyman, "Cybersecurity: Personal information and password setup," *ResearchGate*, 2018. [Online]. Available: https://www.researchgate.net/publication/327571329_Cybersecurity_Personal_Information_and_Password_Setup