

# CYBERAEGIZ: COMPREHENSIVE CYBERSECURITY SUITE

\*Note: Sub-titles are not captured in Xplore and should not be used

Wan Aiman Bin Wan Ibrahim  
Kulliyyah of Information and  
Communication Technology  
Department of Computer Science  
International Islamic University  
Malaysia  
wan.aiman@iium.edu.my

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**— The abstract should provide a clear and concise summary of the Introduction, Literature Review and Methodology (for FYP1) and additional of Results and Conclusion (for FYP2), allowing readers to quickly understand the main points without reading the full document. (*Abstract*)

**Keywords**—any related keywords should be included here

**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.

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

Existing systems were reviewed, and an analysis that highlights both similarities and differences among the systems is included. The similarities and differences could be presented in a table, for easy comparison, as shown in Table 1.

## 2.1 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.

### 2.1.1 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				✓

A comparison 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.

### 2.1.2 Password Management Tools

Feature/Tool	NordPass Password Generator	LastPass Password Generator	Passworden 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				✓

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.

### 2.1.3 Encryption and Decryption Tools

Feature/Tool	DevGlan	Hat.sh	Webbrowsertools	CyberAegiz
Supports Various	✓		✓	✓

Encryption and decryption tools such as DevGlan, Hat.sh, and Webbrowser tools 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.

TABLE I. COMPARISON BETWEEN EXISTING SYSTEMS

Table Head	Table Column Head		
	Table column subhead	Subhead	Subhead
System A	X		
System B	X	X	X
System C			X

A summary of the system adaptation is included after the system review. The summary describes the specific changes and improvements made, explaining how the reviewed systems were used and improved to create the proposed system.

2.2 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 discussion about the selected development approach is included, elaborating on the reasons behind its selection and its relevance to the project (both System Development project and Multimedia project)

Diagrams and explanations related to the system design and database design are included. The system design and database design were clearly explained with the inclusion of supporting diagrams.

Screenshots of the prototype were also included and explained (System Development project) – for INFO 4401 (FYP1) Technical Report only.

Screenshots of the prototype (System Development project) and the storyboard (Multimedia project) are not included in INFO 4402 (FYP2) Technical Report, as the screenshots of the actual project will be provided in the Results section. Please refer to the following section.

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.

IV. RESULTS

This section is only included in the INFO 4402 (FYP2)

Technical Report. This section includes screenshots of the final project,

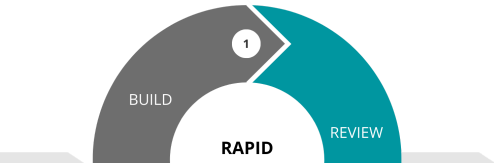
accompanied by explanations. A brief description of the evaluation results is provided within this section.

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.

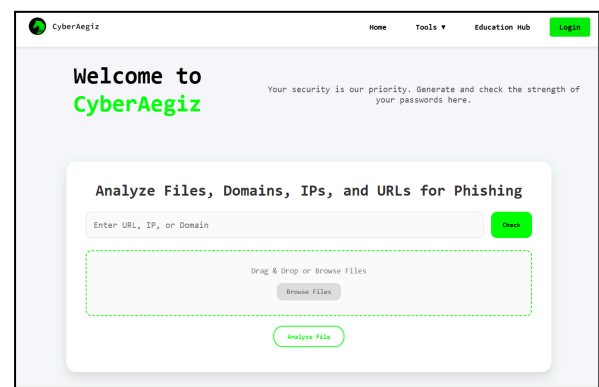
B. System Pages and Functionalities

1. Home Page



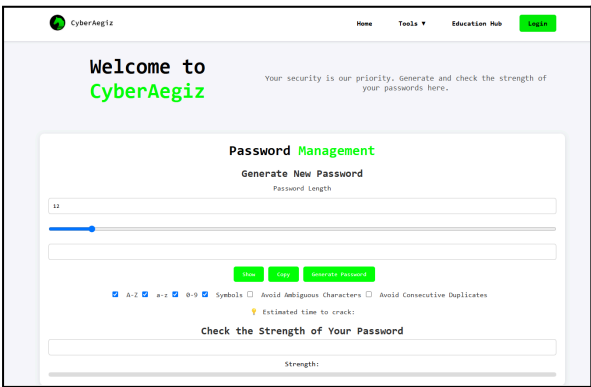
Description: The **home page** welcomes users with an overview of CyberAegiz's features and functionalities. It emphasizes user security and provides quick navigation to different tools.

2. Phishing Detection Tool



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.

3. Password Management Tool



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.

4. Encryption and Decryption Tool



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.

5. Education Hub

Gambar

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.

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] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955. (references)
- [2] [3]
- J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
- [4] K. Elissa, "Title of paper if known," unpublished.
- [5] R. Nicole, "Title of paper with only first word capitalized," *J. Name Stand. Abbrev.*, in press.
- [6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetism Japan, p. 301, 1982].
- [7] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science
- [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](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](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](https://www.researchgate.net/publication/327571329_Cybersecurity_Personal_Information_and_Password_Setup)
- [12] S. M. Kennison and E. Chan-Tin, "Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors," *Frontiers in Psychology*, 2020. [Online]. Available: <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.546546/full>