International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.493

Design and Development of Cybersecurity Suite

Wan Aiman Wan Ibrahim, Ahmad Nazrin Ahmad Khalil, Adamu Abubakar *
Dept. of Computer Science, KICT, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia.

*Corresponding author: adamu@iium.edu.my
(Received: 8th July 2024; Accepted: 25th July 2024; Published on-line: 30th July 2024)

Abstract— Protecting personal, corporate and government data in the digital age requires cybersecurity. Traditional cybersecurity methods sometimes lack comprehensive and dynamic protection mechanisms as cyber-attacks change and become more sophisticated. A new cybersecurity suite is proposed in this study. It integrates various advanced security technologies into a single user-friendly platform interaction. This paper specifically combines techniques for real-time phishing detection, strong password management, safe encryption and decryption services and an interactive module to promote user awareness and behaviours to improve digital security for individuals and organization. Rapid prototyping is used in iterative and incremental development phases to adapt to changing security needs and user input. This method allows the platform to be constantly improved to satisfy the current cybersecurity standards and react to new threats. The prototyped developed provides proactive digital defence, a complete cybersecurity platform that equips users to defend their digital presence. With the intuitive design and advanced feature set, the prototype aspires to democratize cybersecurity. Empirical testing of the prototype revealed that makes an effective protection of a wider audience without the complexities of security software. This paper contributes in the advances cybersecurity technology and shaping the digital protection measures.

Keywords— Cybersecurity, Cybersecurity-suite, phishing detection, password management

I. Introduction

Cybersecurity protects our computers, networks, data and software from threats, unauthorized access, and harm. This broad field protects digital data using numerous methods. It safeguards online-based programmes from unauthorized access, cyberattacks and web environment vulnerabilities. According to Nema and Wally [1]. Integrating cybersecurity prevention framework would address the needs to unified, easy-to-use online application that incorporates numerous cutting-edge security solutions. Specifically, integrating real-time phishing detection, password strength analysis and safe encryption and decryption can improve users' digital security. This is a crucial motivation of this current study. Where it proposed to design and developed an integrated cybersecurity suits.

The motivation of the research lies with cybersecurity protocols, information security and identity management and that each one of these need the other. This is critical in that computer security involves recognising and responding quickly to security threats. According to Buch et al. [2], operational security involves identifying information assets and setting their safeguards. An organization must utilize this method to maintain security. With its thorough security strategy, user-friendly design and instructional features that promote user comprehension, the platform offers several benefits. Dependencies on human interaction, a reliable internet connection and periodic upgrades to manage shifting cyber threats are also challenges. This study aims to safeguard and enable clients against cyber threats. It does this by offering comprehensive cybersecurity solutions at an inexpensive price that allows individuals and small to medium-sized enterprises to readily access them without the complexity of enterprise-level solutions. These criteria are essential for data and system security and monitoring.

In proposing a unified, user-friendly platform that incorporates a suite of advanced security tools, this research 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.

This research also 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. It also strives to provide comprehensive and user-friendly cybersecurity services that enable clients with varying levels

https://doi.org/10.31436/ijpcc.v10i2.493

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.

The present cybersecurity environment is characterized by a fragmented approach to digital threats, with most solutions providing narrow [4]. Moreover, there are isolated defences that do not address the complete spectrum of dangers that users confront. This fragmentation will create substantial holes in defences, especially against phishing, malware and advanced persistent threats, which necessitate a more dynamic and integrated approach. Furthermore, the undoubtedly fast development of cyber threats outpaces standard security product update cycles [5]. Cybersecurity demands a system capable of adapting in real time to emerging problems. The goal is to provide a seamless, scalable and a very simple platform that allows users to simply and efficiently secure their digital assets [6]. Furthermore, the tool is sensitive for independently securing an entire platform. The overriding issue is particularly the integration of these tools and technologies into a unified and accessible application that remains at the forefront of cybersecurity innovation [7]. This will provide effective protection for its users in an ever-changing threat scenario [8].

The rest of this paper is organised as follows: Section 2 present the related work. Section 3 is the methodology. Section 4 is the result and discussion and finally Section 5 is the conclusion.

II. Literature Review

There are many previous research studies that developed cybersecurity suites enabling researchers to explore numerous cybersecurity issues to protect digital spaces. Similarly, this current study, seek to explore and discusses cybersecurity trends, methods and issues from major research. Which enable a clear path to the development of a better cybersecurity suite.

Among the most related previous research is the work of Craigen et al. [9] which proposed a framework to explain digital resource management and preservation. The paper provides the technical solutions and strategic resource allocation to defend cyberspace and its assets against threats that violate property rights. Similarly,

Jain and Gupta [10] examine detection of cybersecurity risk associated to phishing websites. They detect fake sites using visual similarities. Some visual-based solutions are beneficial and should be used in cybersecurity to boost protection. To improve detection, the study advises integrating these methods with machine learning.

Goyal and Khurana [11] study cryptography methods for securing vulnerable network connections. Their research emphasizes secure hybrid cryptographic systems that use symmetric and asymmetric key approaches. Mobile and wireless apps must avoid communication channel issues which increase the security threats. Comparing mobile communications security cryptography approaches is the research method. Combining these technologies may increase security, prompting research into optimizing them for low-power mobile devices.

The 2020 Springer report on Industry 4.0 cybersecurity underlines the prevalence of cyber dangers in online applications and the need for industrial application-specific security protocols. The research tracks cybersecurity threats and advises on digital asset protection using OWASP, NIST and MITRE data. Industry 4.0-specific cybersecurity measures are discussed after analyzing industry reports and guidelines. The study raises important considerations about how security solutions can adapt to constantly changing industrial technologies.

Nema BM, Wally [1] established that SQL injection attacks, being the key site security concern in 2019, requires a lot concern. The paper recommends multi-connect architecture to identify and mitigate hazards. Web application security is improved via SQL injection detection and remediation. As the study concludes and may fix a recurring issue, web developers must use advanced security measures like the recommended way in their apps.

Sarker et al. [12] established that cybersecurity data science from an overview of machine learning might improve the entire cybersecurity prevention. This research links theoretical data science applications to real cybersecurity solutions by examining machine learning algorithms for cyber threat prediction and mitigation. According to studies, cyber dangers are complicated making these creative methods difficult to apply. More empirical research is needed to confirm these theories which shows increased interest in AI and machine learning in cybersecurity is highly appreciated. Typically, machine learning techniques applied to cybersecurity dwells on how machine learning can improve cybersecurity. Despite the study of examines machine learning methods and how they may help cybersecurity issues are not certain. Sarker et al. [12] recommends strategies to increase digital security but it calls for more empirical research to test these techniques in real life. The gap between theoretical understanding and real implementation must be closed to produce more robust cybersecurity solutions.

According to Goyal et al. [13], cybersecurity risks and countermeasures covers all current web application cybersecurity concerns and offers remedies. The report's detailed analysis includes recent cybersecurity events and provides an up-to-date threat picture. The paper uses a systematic review technique to evaluate hazards and give cutting-edge solutions revealing the ever-changing nature of web application security. The paper is acclaimed for its comprehensiveness and timeliness but it recognises the need for regular revisions to stay relevant. Because the it

https://doi.org/10.31436/ijpcc.v10i2.493

recognises the rapid rise of technology and cyber methods in the digital world.

Ma et al. [14] established that Personal Information and Password Setup requires people's knowledge of the significance of protecting their personal information affects their password strength. The paper uses a mixed-method approach to perform a thorough research. The surveys part of the research assesses participants' awareness of password security and personal data protection. The finding indicate that security awareness improves password strength. Similarly, the other part of the study shows that security-savvy people choose stronger passwords to that do not associated to the age, and other demographic variables.

Kennison and Chan-Tin [15] revealed that "Taking Risks with Cybersecurity" requires using knowledge and personal characteristics in order to predict self-reported cybersecurity behaviours. That is why the study examines how cybersecurity knowledge and personal traits affect password security. The study employed a quantitative methods and assess participants' cybersecurity knowledge and behaviour. The findings indicate that knowledge, personal traits and reported practices increased cybersecurity expertise leads to enhanced safety processes according to the study.

Following an extensive review of all the previous research studies highlighted. This current research was able to extract a single research gap that is very crucial to the computing community. That is, there is a lack of consolidating cybersecurity preventive measures in majority of the research reviewed. Despite the awareness of different cybersecurity issues, yet the solutions are not provided in a consolidated approach. That is why this current study design a unified cybersecurity platform that integrates essential web and data security tools and develop a prototype suite of the essential security tools, including phishing detection, password strength analysis, encryption/decryption services and a password generator, along with an educational component focused on enhancing users' cybersecurity knowledge and practices.

III. Materials and Methods

This study relied on the formal software development process flow to design, develop and test a prototype of the cybersecurity suite. Specifically, rapid prototyping software development approach was adopted, which tests product functionality, designs and usability. This was done by quickly creating and revising prototypes. This kind of development require regular feedback and adaptation benefit, that is one of the reason for the selection of the approach. Since developers can quickly discover and fix design problems and user requirements makes rapid prototyping a suitable technique to follow.

A. System Design

The proposed system design for this study is presented in Figure 1. The system comprises of three layers as follows:

1. Application Layer:
2. Control Layer
3. Infrastructural layer

The Application Layer involves direct connection with end-users and includes crucial components such as: The Net Infrastructure like the Security APIs and the "System interfaces" for authentication and authorization. Similarly, the layer contents the "content delivery Network" that optimises worldwide content delivery and reducing bandwidth and load times. The layer is also responsible for "Balancing load" as well as spreading network or application traffic across numerous servers for stability and availability. Within this layer, there is a provision of "Firewall" which is essential for security technologies that filter network traffic according to security requirements. Similarly, this research constructs a firewall between a trusted internal network and an untrustworthy external network like the internet to prevent threats and unauthorized access.

The proposed design consider the "User Interfaces" to be part of the "Application layer", where the "End-User Interface" is structured. Crucial to this is the "Normal users" views are set to utilize the front end to inspect URLs or receive phishing alerts and also utilize other tools. Furthermore, the "Admin Screen" is conceptualized to manage users, configure settings and also examine analytics an all-user interface that may incorporate instructional materials and personal settings are the last part of this group.

The "Control Layer" was conceptualized to be responsible for the system's core logic and processing where the "Web Server" which serves as the static material or forwards user interface requests to the application server for dynamic content. Similarly, the "Application Server" is part of the control layer, where it manages all the complicated back-end activities and transactions. Third-Party Services (APIs) involving external and integrated services for data verification and additional information are also set out to be in this layer. Within the control layer, an "Encryption/Decryption Module" that provides users with tools to securely encrypt and decrypt their sensitive data are set out. There is also a provision, of Password Management Module: Generate customizable passwords and password strength checker with crack time estimation.

The next within this layer is the "Phishing Detection Module" where the fundamental component that checks URLs and other content for phishing are set out. Finally, the educational module that provides for an interactive or informational contents on cybersecurity education.

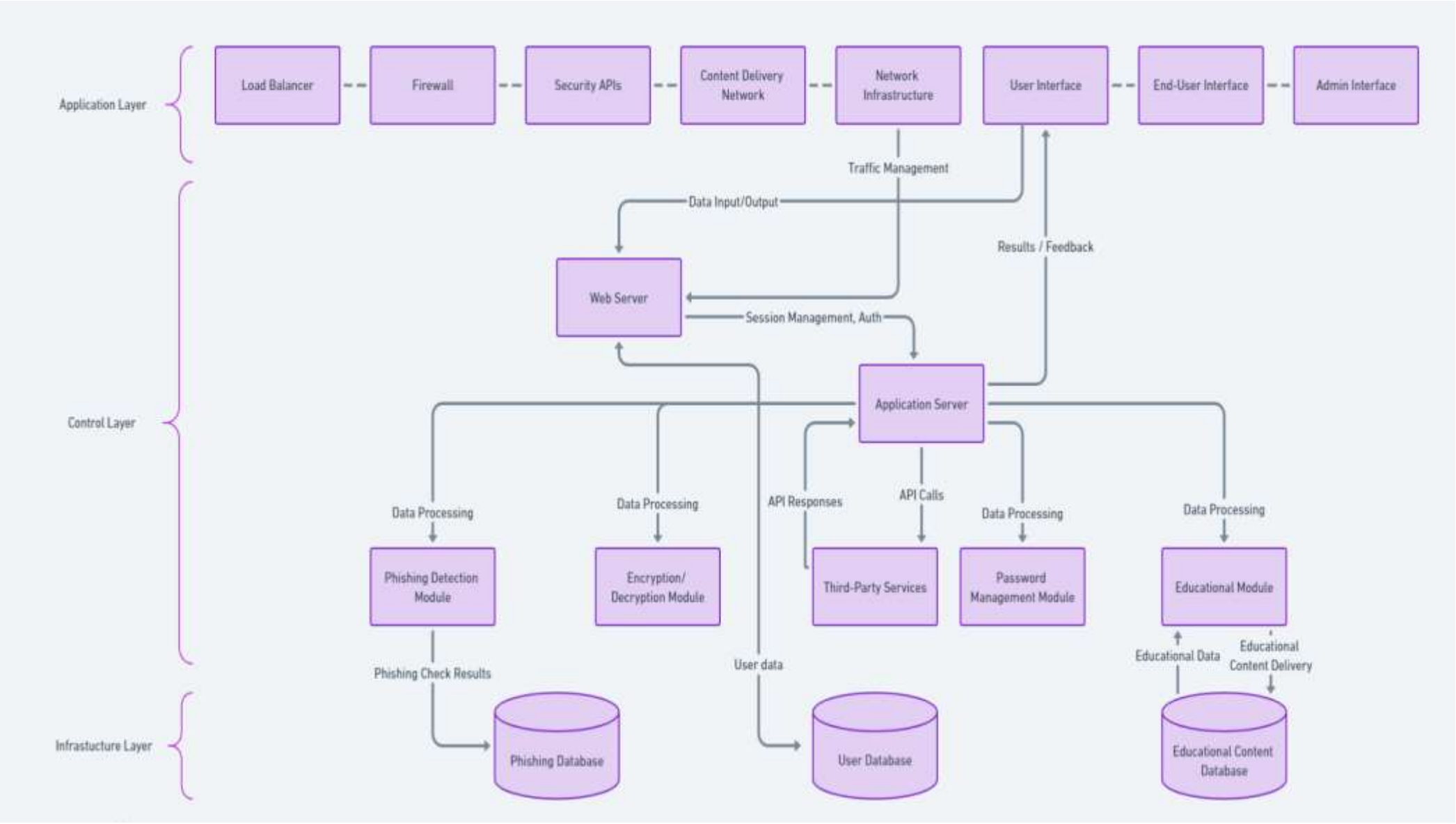

Fig 5. The Entire System Design

The last layer is the "Infrastructure Layer" this layer provide all the necessary computational operations defined for the infrastructure required. The layer provides data and content storage for the entire system. This is typical to the "Phishing Database" where it stores the identified phishing attempts, sites and disputed phishing results. Similarly, within the layer, there is a provision for "Educational Content Database" which search as the "Contains of quiz", "lessons", "videos", and other content for the Educational Module.

The three layers can be best describe as the functional layers, where "data Flow" from the users submitting to the URLs and access instructional content through various interfaces. Web servers handle requests and application servers will process them. The relevant modules analyse URLs, offer content and maintain passwords. The databases store the findings or content. The security and performance module handle the security APIs, CDNs and Load Balancers lock down the system. It will also handle excessive traffic and distribute content efficiently. Finally, the modularity of the architecture separates all the functions into modules for scalability and maintainability. This make it easy to update or modify one element without affecting others. This systematic approach makes the system strong, scalable, easy to manage, secure and user-friendly.

B. *Use Case Scenarios of the system*

There are four use case scenarios of the system proposed in this study (see Figure 2) "Use Case Scenario of Phishing Detection Tool", "Use Case Scenario of Password Management Tool", "Use Case Scenario of Encryption and Decryption Tool", and "Use Case Scenario of Cybersecurity Education Section".

The first use case associated to Phishing detection scenario start with the first action that lies with "Precondition": 1) The user has access to the phishing detection website. 2) The phishing detection system and database are operational.

The second case involve the "Main Flow". The first of this lie with the "User Enters URL/Domain/IP/File". In this case, the phishing detection website asks users to enter or upload URLs, domain names, IP addresses and files. Then follow by the user input the URL/domain/IP/file for analysis. The next action involves "System Processes Submission". The system processes the submission using phishing detection APIs. The detection mechanism evaluates the submission against a database of known phishing sites. After that, the next action is "User Receives Result" that is after examination, the system shows and alerts the user if the URL/domain/IP/file is safe or suspicious/phishing. The next action involves "Update Database". That is If the submission is identified as a new phishing threat, the system automatically updates the phishing database with this new information. This procedure may save URL, information and detection parameters.

The third case involves "Alternative Flow" where the first action is "User Disputes Result". That is, if they disagree with the detection result, users can dispute it. The user can provide feedback or explanations for the inaccurate result. Based on this feedback, system administrators may update the database. The next action that follows involves "Downloading Extension". The user can download a real-time phishing browser extension at any moment. The extension will automatically flag questionable URLs during browsing.

The final case associated to phishing is "Post conditions" where the first action involves the phishing database updating any new findings or corrections. The user will have a clearer understanding of the safety of the URL/domain/IP or file.

Considering that password management and systems hold an important concern. The "Use Case Scenario associated to Password Management Tool" Involve similar flow with the Phishing detections except that the "Precondition" is that the password management tools are accessible and operational on the website. The Admins have established initial password policies and algorithms.

Hence the "Main Flow" is associated to the "User Enters Criteria" where "User input criteria for a new password. Length, complexity (numbers, symbols, etc.) and preferences may be considered". The "Receives New Password" is the system that produces a password that meets the conditions. where "Users see their updated password", Receives Tips / Feedbacks, along with the new password, the system offers password strength tips and advice on building stronger passwords. Similarly, the regenerate New Password (Extension)

offer Users can regenerate passwords if they are unhappy with the generated ones. The system generates a new password using the same or updated criteria.

The Alternative Flow provide "User Inputs Password" In a different scenario, the user inputs any password into the system for validation. Receive Tips/Feedbacks on the system which evaluates the password and offers solutions for strength, security and improvement. In the "Postconditions", "Users receive strong passwords and password security advice" Then the action involve "Keeping password policies and algorithms current with best practices ensures user security.

https://doi.org/10.31436/ijpcc.v10i2.493

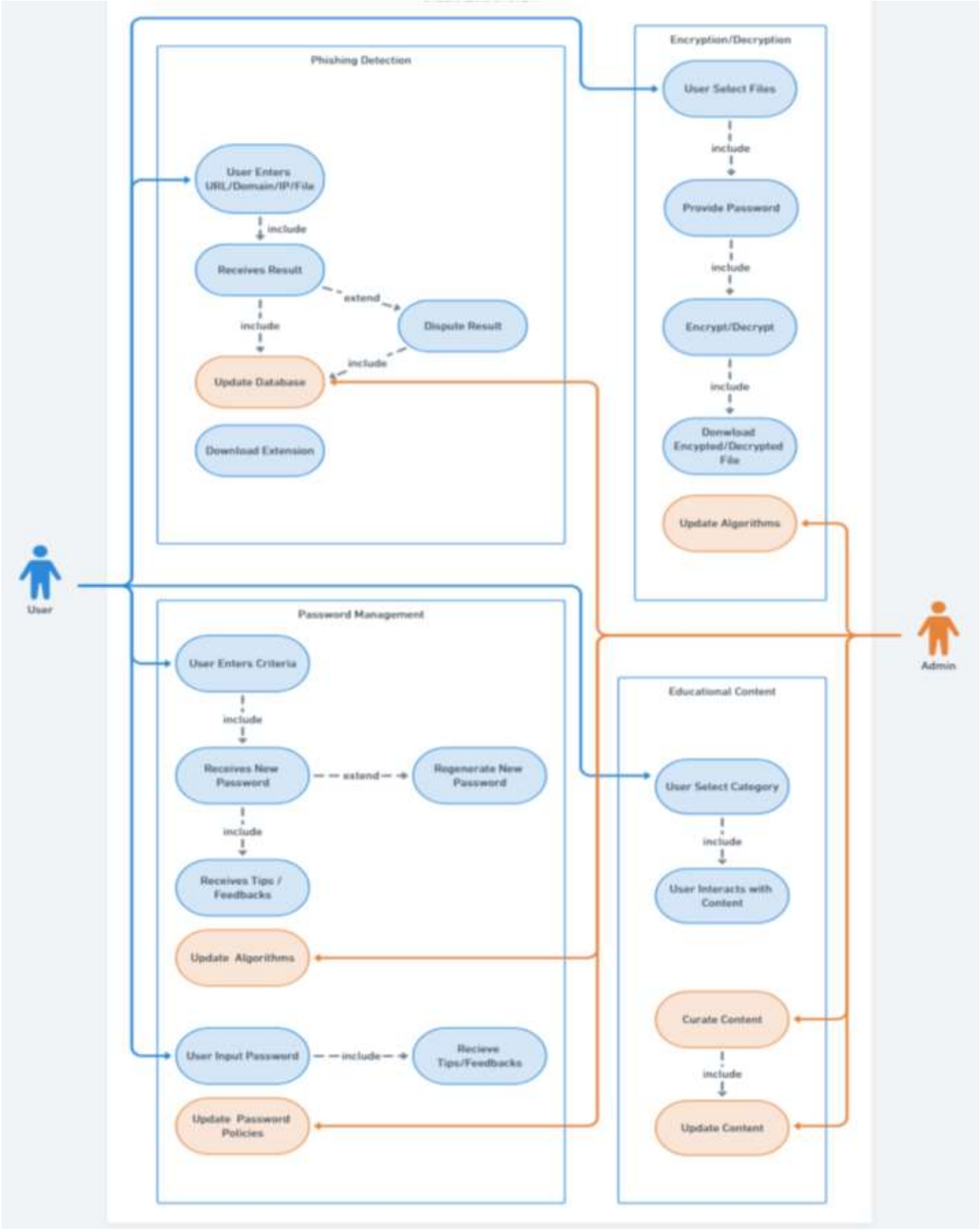

Fig. 2 The Use Case Scenarios of the Functional Flow

https://doi.org/10.31436/ijpcc.v10i2.493

The "Use Case Scenario associated to Encryption and Decryption Tool" provide that the

"Precondition" is the user has access to the encryption/decryption interface on the website. The encryption/decryption algorithms are correctly implemented and functional. The "Main Flow" involve "User Selects Files", Users visit the website's encryption/decryption area. The interface lets users submit files to encrypt or decrypt.

The "Provide Password" action initiated After selecting the files, the user must input a password for encryption or decryption. The key encrypts data and restricts access to them. the Encrypt/Decrypt action was initiated after entering the password, the user chooses to encrypt or decrypt files. The system processes files using the password and current encryption/decryption techniques.

The "Download Encrypted/Decrypted File" Initiated after encryption or decryption, the system lets users download the file. User can download encrypted or decrypted file to local device for use. Finally, the "Alternative Flow" lead the. System or Password Error, If the encryption/decryption procedure fails (e.g., wrong password), system will notify user and may demand for password re-entry or file upload retry. The "Postconditions" lead The files are encrypted or decrypted as requested by the User.

The final "Use Case Scenario" is associated to "Cybersecurity Education Section". The "Precondition" involves the educational content system that is operational and accessible through the website. The content is well-organized into categories. The "Main Flow" lies with the "User Selecting Category" associated to "Users visit Educational Content on the website. Users choose a category based on their interests. The "User Interacts with Content" only after choosing a category, users see articles, videos, tutorials and interactive quizzes. Reading, watching and interacting with material engages users. The "Postconditions" involves the Latest and reliable information is updated in the educational material database. Updated and selected content keeps users aware about phishing and cybersecurity

IV. Results

The system designed provided in the previous section has now been implemented. The result of the system flow is presented in this section. The First user interface of the system is presented in Figure 3. It provides a form features that is a very basic and simple form with clear input boxes for Email/Username and Password. This is accompanied by "Supportive Options" that includes links for registering or recovering passwords. This can provide a smoother user experience and accessibility.

Fig. 3 The First User Interface of the system

The next is the "Extended Form Features" (see Figure 4) where it provides an Identical to the login screen but with a password confirmation area. It ensures users set credentials safely and correctly. This is followed by "Guide for Users" involving a "Very clear instructions" and error handling could improve registration by ensuring users enter proper information.

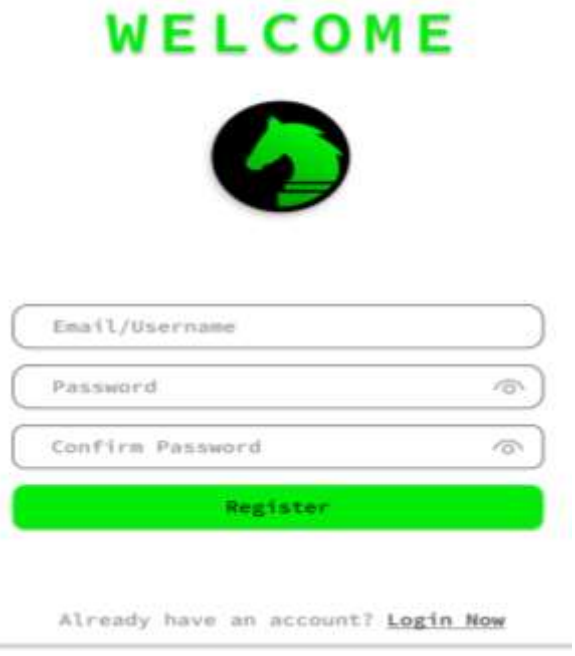

Fig. 4 The registration Confirmation Stage

Figure 5 present the main dashboard after an entry to the system. The dashboard is called "CyberAegiz". It involves a

https://doi.org/10.31436/ijpcc.v10i2.493

"Header and Navigation" where the top portion has the website's logo on the left, centrally oriented navigation buttons for "Home", "Tools" and "Education Hub" on the right, and a search box. The site is easy to navigate with this layout. The Main Content Area involves "A greeting message" with a vivid background and a cybersecurity-focused graphic. Below this are clickable tiles for "Phishing Detection", "Password Management", "Encryption & Decryption" and "Education Hub". The icons and brief descriptions on each tile explain each tool. The "Call to Action" involves a big "Learn More" button urges CyberAegiz users to explore its features. Finally, the "Footer" includes links to "About Us", "Privacy Policy", "Terms of Use" and "Contact Us", which are essential for website credibility and user support.

Fig. 5 The System ROC Curve for Naive Bayes with BOW

The phishing detection module functionality involve a system will scan URLs or uploaded files against a phishing database. The real-time phishing scanning extension is optional to download. Results Interface: Results will show a short summary of the URL status whether it is "Good" or "Suspicious". Educational Section: Teach people about phishing and protection techniques. This can promote safer browsing experiences.

The password management "Dual Functionality" combines password generator with strength checker. Users can customize password restrictions and receive real-time password strength feedback. The Interactive Elements involves the screen has sliders and toggles to define password parameters and visual indicators of user-generated or typed password. An advice and tips section provides practical guidance on building and keeping strong passwords for online security.

The Encryption and Decryption involves "Tool Operations" that involve "A drag-and-drop" or file selection interface simplifies encryption and decryption. Encrypted files are secure with passwords. Process Visualization: After encryption, users can download encrypted files with clear instructions and visual signals. Best Practices: Promotes encryption and provides instructions for safely managing encryption keys and protecting sensitive data.

The Educational model provide the "Read Articles". Many cybersecurity articles are available. Articles may cover broad knowledge, detailed guidelines or best practices. The tabs "All Articles," "General Guides," and "Cybersecurity Practices" enable readers to find articles based on their interest or ability level. Learning Through Multimedia: Articles with several photos may include multimedia features like films, infographics or interactive diagrams to enhance comprehension of sometimes very difficult cybersecurity issues. Interactive Quizzes or Assessments: Educational hubs may feature interactive quizzes or assessments. This could help to test readers' grasp of the topic. It can help retain knowledge and apply theoretical concepts.

V. Conclusion

This paper presents a design and development process emphasizing on rapid prototyping over extensive four cybersecurity modules. The development was performed base on the proposed designed intended to integrated cybersecurity feature into a single dashboard. The prototyped developed is called "CyberAegiz". It was tested and the result guarantee that the suit fit the user expectations and handle cybersecurity concerns. CyberAegiz benefits from rapid prototyping for various reasons. It integrates user and community insights with constant feedback. Feedback is essential for improving the application's functionality and usability and creating effective tools. Cyber threats are dynamic; thus a quick adaptation is very important. The rapid prototyping enables for any design changes. These are definitely necessary for integrating new cybersecurity defenses or responding to new vulnerabilities. The prototyping eliminates the need for major adjustments later in the development process. This optimize resource allocation and minimize lost effort. The outcome of the research can be used in a real-world difficulties and iterative feedback, improving learning style.

Acknowledgment

This research is supported by UMP-IIUM Sustainable Research Collaboration 2022 Research Grant (IUMP-SRCG22-014-0014).

Conflict of Interest

The authors declare that there is no conflict of interest.

References

[1] M.B. Nema, Wally HA. Cybersecurity risks detection and prevention. Al-Mansour Journal. 2019;31(1):65-86.

[2] R. Buch, Ganda D, Kalola P, Borad N. World of cyber security and cybercrime. STM Journal., 2017, 4(2),

[3] I.H. Sarker, Kayes AS, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big data. 2020 Dec; 7:1-29.

[4] C. Florackis, Louca C, Michaely R, Weber M. Cybersecurity risk. The Review of Financial Studies. 2023 Jan 1;36(1):351-407.

[5] D.W. Hubbard, Seiersen R. How to measure anything in cybersecurity risk. John Wiley & Sons; 2023 Apr 11.

[6] B. Gumaida, Ibrahim AA. IWDSA: A Hybrid Intelligent Water Drops with a Simulated Annealing for The Localization Improvement in Wireless Sensor Networks. Int. J. Appl. Inf. Technol. Vol. 2024;8(01):15.

[7] B.T. Familoni. Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. Computer Science & IT Research Journal. 2024 Mar 22;5(3):703-24.

[8] A. Almuqren, Alsuwaelim H, Rahman MH, Ibrahim AA. A Systematic Literature Review on Digital Forensic Investigation on Android Devices. Procedia Computer Science. 2024 Jan 1; 235:1332-52.

[9] D. Craigen, Diakun-Thibault N, Purse R. Defining cybersecurity. Technology innovation management review. 2014;4(10).

[10] A.K. Jain, Gupta BB. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks. 2017;2017(1):5421046.

[11] R. Goyal, Khurana M. Cryptographic security using various encryption and decryption method. International Journal of Mathematical Sciences and Computing (IJMSC). 2017;3(3):1-1.

[12] A.A. Alarood, Ibrahim AA, Alsubaei FS. Attacks Notification of Differentiated Services Code Point (DSCP) Values Modifications. IEEE Access. 2023 Nov 13;11:126950-66.

[13] D. Goyal, Lavania G, Sharma G. Review of modern web application cybersecurity risks and counter measures. InAIP Conference Proceedings 2023 Jun 15 (Vol. 2782, No. 1). AIP Publishing.

[14] Y. Ma, Twyman, Nathan W., "Cybersecurity: Personal Information and Password Setup" (2018). MWAIS 2018 Proceedings. 20.

[15] S.M. Kennison Chan-Tin E. Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology. 2020 Nov 4;11:546546.