Journal of Informatics and Web Engineering

Vol. 3 No. 3 (October 2024) eISSN: 2821-370X

Enhancing Cybersecurity Awareness through Gamification: Design an Interactive Cybersecurity Learning Platform for Multimedia University Students

Adlil Khaliq bin Abdul Razack[1], Mohamad Firdaus bin Mat Saad[2]

[1,2] Faculty of Computing and Informatics, Multimedia University, Malaysia
**corresponding Author: (firdaus.matsaad@mmu.edu.my, ORCiD: 0000-0003-3768-4808)*

Abstract - Cybersecurity has emerged as a critical imperative in contemporary digital landscapes, necessitating heightened awareness and proficiency across all demographic segments. Accordingly, this research has been meticulously crafted to delve into the complexities of cybersecurity awareness, with a specific focus on university students. The study embarks on an exhaustive analysis encompassing the evaluation of cybersecurity awareness levels within the targeted groups, the identification of prevailing issues and practices, and an exploration of novel methodologies, notably gamification, to fortify cybersecurity knowledge and skills among diverse user cohorts. Central to this investigation is the efficacy of gamified learning environments tailored expressly for augmenting cybersecurity awareness among university students. Through a comprehensive examination of existing platforms, methodological frameworks, and user interactions, this research outlines critical trends, challenges, and latent opportunities within the cybersecurity awareness domain, with a specific emphasis on gamification's transformative potential. The study not only identifies key areas for improvement but also proposes innovative solutions rooted in gamified learning paradigms, with the overarching goal of fostering engaging, effective, and sustainable cybersecurity awareness initiatives among students. Drawing upon a synthesis of theoretical constructs, empirical insights, and pragmatic recommendations, this research significantly contributes to the evolving discourse on cybersecurity education. By underscoring the transformative efficacy of gamification as a pivotal tool in cybersecurity awareness initiatives, this study overlays the way for substantial advancements in cybersecurity education paradigms, offering a roadmap for enhancing cybersecurity awareness levels among university students and beyond.

Keywords- Cybersecurity Awareness, Gamification Education, Cyber Threats, Transformative Learning, Cybersecurity Platform

Received: 28 April 2024; Accepted: 28 June 2024; Published: 16 October 2024

1. INTRODUCTION

The contemporary digital landscape accentuates the critical importance of cybersecurity, a vital shield against escalating cyber threats targeting individuals, corporations, and governmental entities. Within this context, students emerge as a demographic particularly vulnerable to cyber risks, often navigating digital technology without adequate awareness or skills to mitigate potential dangers effectively [1]. This vulnerability exposes them

Journal of Informatics and Web Engineering
https://doi.org/10.33093/jiwe.2024.3.3.2
© Universiti Telekom Sdn Bhd.
Published by MMU Press. URL: https://journals.mmupress.com/jiwe

to various threats such as identity theft, data breaches, and other virtual hazards, highlighting the urgent need for comprehensive cybersecurity education and training [2].

Real-world incidents, exemplified by the recent data breach at seven Idaho colleges, serve as stark reminders of the repercussions of inadequate cybersecurity measures [3]. This breach compromised sensitive personal information due to vulnerabilities in third-party software, emphasizing the pressing need to bridge the cybersecurity knowledge gap among students and provide them with the necessary tools to navigate the digital realm securely.

To address this challenge, innovative approaches are essential, including gamification, which integrates game elements into educational contexts to enhance motivation, engagement, and learning outcomes [4]. By infusing the learning process with interactivity, rewards, feedback, challenges, and incentives, gamified platforms have the potential to stimulate curiosity, foster creativity, and cultivate a culture of cybersecurity consciousness among learners.

The primary focus of this research paper is to propose a gamification platform dedicated to cybersecurity awareness for MMU students. This web-based application will offer a comprehensive suite of cybersecurity topics, interactive quizzes, engaging games, and achievement badges, supported by performance tracking capabilities for students to monitor their progress and interact with peers and instructors. Rooted in effective gamification design principles, including clear objectives, meaningful choices, timely feedback, and social interaction, this platform aims to significantly contribute to the cybersecurity education domain by fostering a proactive approach to cybersecurity among students.

Structured into four main sections, this paper will begin with an in-depth analysis of current practices in cybersecurity education, exploring prominent platforms such as CyberPatriot, Proofpoint Security Awareness Training, and Cisco Secure Awareness Training. Subsequently, it will delve into the challenges faced by these platforms, engage in an open discussion on potential solutions and enhancements, and conclude with a forward-looking discussion on directions for cybersecurity education and training proposed platform.

2. LITERATURE REVIEW

In today's digital age, cybersecurity has emerged as a paramount concern, especially within the context of university education [5],[6]. University students, being avid users of digital technologies, face unique cybersecurity challenges that require attention and proactive measures. This scientific review delves into the various facets of cybersecurity challenges from the perspective of university students, highlighting key issues, trends, and potential solutions to enhance cybersecurity awareness and practices among this demographic.

One of the fundamental challenges faced by students is the management of their digital footprint and privacy concerns [7]. With extensive engagement in social media, online banking, and academic platforms, students accumulate a significant digital presence, making them vulnerable to privacy breaches, identity theft, and unauthorized access to personal information. Heightened awareness and adoption of privacy-enhancing practices are essential to mitigate these risks effectively.

Phishing and social engineering attacks pose another significant threat to university students' cybersecurity [8], [9], [10]. Cybercriminals leverage deceptive emails, messages, and social media posts to trick individuals into divulging sensitive information or clicking on malicious links. Students' lack of awareness regarding phishing techniques and the importance of source verification contributes to their susceptibility to these attacks, necessitating robust education and training on identifying and avoiding phishing attempts.

Insecure Wi-Fi networks on university campuses also expose students to cybersecurity risks [11]. Public Wi-Fi networks, often unsecured, are susceptible to interception by malicious actors, compromising the confidentiality of data transmitted over these networks. Coupled with students' reliance on personal devices such as laptops, smartphones, and tablets, inadequate device security measures further exacerbate the risk of security breaches. Implementing secure Wi-Fi protocols, promoting the use of VPNs, and educating students on device security best practices are crucial steps in mitigating these vulnerabilities.

Ethical considerations and cyber ethics also play a pivotal role in cybersecurity education for university students [12]. Upholding academic integrity, avoiding plagiarism, cheating, and unauthorized access to academic resources are essential ethical norms that students must adhere to. Integrating cyber ethics education into the curriculum fosters a culture of responsible online behaviour and digital citizenship among students, contributing to a safer and more ethical digital environment.

The transition to remote learning during the COVID-19 pandemic brought about additional cybersecurity challenges for university students [13], [14], [15]. Concerns about the security of virtual learning platforms, video conferencing tools, and online collaboration tools heightened the importance of ensuring the confidentiality, integrity, and availability of online learning resources. Universities must invest in secure online platforms, provide cybersecurity training for students and faculty, and implement robust security protocols to safeguard the integrity of remote learning environments.

Cybersecurity education and training programs tailored for students are indispensable in equipping them with the knowledge and skills to navigate the digital landscape securely. Integrating cybersecurity into the curriculum, offering workshops, and conducting cybersecurity awareness campaigns are effective strategies to empower students to identify cyber threats, secure their devices and data, and respond effectively to security incidents. Collaboration between universities, students, and cybersecurity experts is key to developing comprehensive cybersecurity strategies that address the evolving threats faced by students.

3. EXISTING SYSTEMS REVIEW

In the evolving landscape of cybersecurity education, existing platforms like CyberPatriot, Proofpoint, and Cisco Secure Awareness Training have established benchmarks for engaging and educating users. These systems utilize a variety of techniques, including competitive challenges, interactive training modules, and phishing simulations, to enhance cybersecurity awareness. However, each platform has its distinct focus, audience, and limitations, particularly in terms of personalization, gamification, and accessibility for educational institutions. This project acknowledges the strengths and gaps in these existing solutions, aiming to tailor a more engaging, accessible, and comprehensive cybersecurity awareness platform specifically designed for students. By integrating personalized learning paths and gamified elements, the proposed system seeks to address the unique needs of the student body, fostering a deeper understanding and proactive approach to cybersecurity.

3.1. CyberPatriot

CyberPatriot, created by the Air Force Association, targets students aged 13 to 21 to develop their cybersecurity skills through competitive virtual cyber ranges and hands-on learning experiences [16]. While it promotes problem-solving, critical thinking, and career exploration opportunities, it faces challenges such as resource-intensive contests, access barriers, program complexity, and inclusivity issues. Enhancements in funding, mentorship, accessibility, curriculum diversity, and quality assurance are essential to ensure CyberPatriot remains an effective tool for cybersecurity education.

3.2. Proofpoint

Proofpoint's Security Awareness Training platform offers interactive modules, phishing simulations, personalized training paths, and comprehensive reporting for cybersecurity education [17]. Despite its extensive features, Proofpoint encounters challenges related to complexity, cost-effectiveness, threat intelligence, user training, and customer service. Simplification, system compatibility, pricing strategies, customer support improvements, and efficient training programs are critical for overcoming these hurdles.

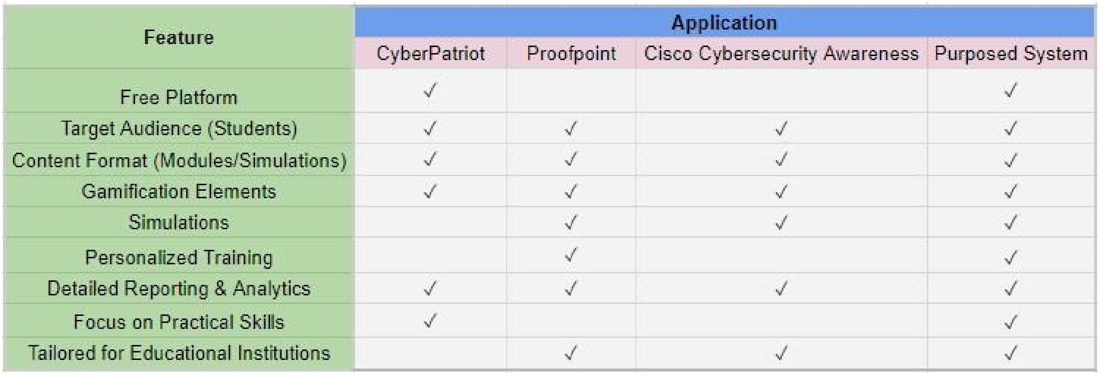
3.3. Cisco Secure Awareness Training

Cisco's platform provides a pre-built content library, customization options, engaging delivery methods, simulated phishing attacks, and comprehensive reporting [18]. Challenges include participant engagement, content relevance, scalability, behaviour assessment, accessibility, cultural adaptation, and policy alignment. Enhancements in accessibility, content relevance, innovation in delivery methods, frequent updates, inclusivity, and policy compliance are necessary to optimize Cisco's Cybersecurity Awareness program.

While these platforms contribute significantly to cybersecurity education, addressing their limitations through enhancements in accessibility, personalization, gamification, content relevance, inclusivity, and cost-effectiveness is crucial. Tailoring cybersecurity education platforms to meet the specific needs and preferences of students requires a strategic approach that leverages the strengths of existing systems while innovating to overcome their shortcomings, ultimately contributing to a more effective and impactful cybersecurity awareness program.

The comparison and analysis presented in Table 1 shed light on the strengths and limitations of existing cybersecurity education platforms, namely CyberPatriot, Proofpoint, and Cisco Cybersecurity Awareness. This assessment serves as a foundation for identifying key deficiencies and opportunities for improvement within these platforms, paving the way for the development of more effective and tailored solutions. By critically evaluating the features and functionalities of these platforms, the author managed to pinpoint areas that require enhancement and innovation to meet the evolving needs of cybersecurity education, particularly from a student-centric perspective.

Table 1. Existing Systems Comparison



Feature	Application			
	CyberPatriot	Proofpoint	Cisco Cybersecurity Awareness	Purposed System
Free Platform	✓			✓
Target Audience (Students)	✓	✓	✓	✓
Content Format (Modules/Simulations)	✓	✓	✓	✓
Gamification Elements	✓	✓	✓	✓
Simulations		✓	✓	✓
Personalized Training		✓		✓
Detailed Reporting & Analytics	✓	✓	✓	✓
Focus on Practical Skills	✓			✓
Tailored for Educational Institutions		✓	✓	✓

In Table 1, the comparison underscores notable shortcomings in current cybersecurity education platforms. Current cybersecurity education platforms, such as CyberPatriot, Proofpoint, and Cisco Cybersecurity Awareness, have numerous shortcomings when used in educational contexts like Multimedia University (MMU). Personalized learning pathways, which are necessary to meet the various learning needs of students, are frequently absent from these platforms. Moreover, they frequently concentrate on business settings, which might not be in line with MMU's educational goals. Furthermore, the majority of these systems lack adequate gamification, a crucial component that is proven to improve learning outcomes and student engagement. Cost is another major obstacle since organizations with tight resources might not be able to afford these premium services. These drawbacks emphasize the demand for more specialized, interesting, and reasonably priced cybersecurity education programs in academic settings.

This comparison further explores their features based on criteria such as interactive modules, quizzes, challenges, leaderboards, badges, storytelling, social interaction, progress tracking, accessibility, user engagement, and customization as presented in Table 2. By examining these aspects, we can better understand how each platform leverages gamification to educate and motivate users in cybersecurity practices. The following table provides a detailed comparison of these platforms, highlighting their unique strengths and capabilities.

Table 2. Comparison of CyberPatriot, Proofpoint, and Cisco Secure Awareness Training Based on Gamification Awareness Criteria

Criteria	**CyberPatriot**	**Proofpoint**	**Cisco Secure Awareness Training**
Interactive Modules	High interactivity with simulated scenarios and challenges.	Moderate interactivity, focusing on real-world phishing simulations.	High interactivity with various learning modules and simulations.
Quizzes and Assessments	Regular quizzes and assessments to track progress.	Frequent quizzes integrated into email simulation exercises.	Comprehensive quizzes at the end of each module.

Challenges and Competitions	National competition structure with various challenges.	Limited competitive elements, primarily focused on individual performance.	Periodic challenges to reinforce learning, no large-scale competitions.
Leaderboards	National and regional leaderboards to encourage competition.	No public leaderboards; performance tracking is private.	Leaderboards within organizations to foster internal competition.
Badges and Rewards	Earn badges and recognition for completing challenges.	Some badges for completing modules, but less emphasis on rewards.	Badges and certificates awarded for course completions and milestones.
Storytelling and Scenarios	Uses engaging scenarios related to cybersecurity threats.	Real-world email threat scenarios.	Scenario-based learning modules to contextualize threats.
Social Interaction	Team-based challenges promoting collaboration.	Primarily individual-based, with some group activities.	Opportunities for team-based activities and discussions.
Progress Tracking	Detailed progress tracking and reporting.	Comprehensive tracking with emphasis on individual improvement.	In-depth tracking and analytics for user performance.
Accessibility	Accessible through various devices, including mobile.	Accessible on desktop and mobile platforms.	Accessible via multiple devices, ensuring flexibility.
User Engagement	High user engagement through competitive and interactive elements.	Moderate engagement through personalized phishing simulations.	High engagement with diverse learning methods and interactive content.
Customization	Customizable to fit different educational needs and levels.	Limited customization options, mainly focused on phishing.	Highly customizable to fit organizational needs and user levels.

The identified deficiencies underscore the need for innovative solutions that bridge these gaps and offer a comprehensive, student-centric cybersecurity education platform. The proposed systems will address these shortcomings by incorporating essential features such as phishing simulation, personalized training paths, practical skills development modules, and tailored educational content. Moreover, enhancements in accessibility, inclusivity, and user engagement will be prioritized to ensure a holistic and effective learning experience.

By integrating these critical functionalities and refining existing features, the proposed systems aim to set a new standard in cybersecurity education, catering specifically to the needs of students and educational institutions. This strategic approach aligns with current research trends and contributes significantly to advancing the field of cybersecurity education by offering a more tailored, interactive, and impactful learning environment.

4. OPEN DISCUSSION

The contemporary digital landscape not only underscores the urgent necessity for robust cybersecurity education but also highlights the dynamic nature of cyber threats and the evolving tactics employed by malicious actors. Recent reports from cybersecurity agencies and industry experts reveal a significant surge in cyberattacks targeting educational institutions, with notable incidents such as the 2021 ransomware attack on a major university resulting in substantial data breaches and operational disruptions [19], [20]. These real-world incidents serve as stark reminders of the critical need to fortify cybersecurity measures and enhance educational initiatives to safeguard sensitive data and infrastructure.

In response to the escalating cyber threat landscape, innovative strategies such as gamification have gained traction as effective tools to elevate cybersecurity education [4]. Research studies, highlights the efficacy of gamified approaches in promoting active learning, improving retention rates, and fostering behavioural changes among learners [21]. The integration of game elements such as interactive scenarios, virtual simulations, and gamified assessments not only enhances student engagement but also cultivates a deeper understanding of cybersecurity concepts and best practices [22].

The proposed gamification platform is designed based on scientific principles and empirical research findings in gamification and cybersecurity education. Drawing insights from cognitive psychology and learning theories, the platform employs adaptive learning algorithms to personalize content delivery and assessments based on students' proficiency levels and learning preferences. Furthermore, the platform incorporates gamification mechanics such as progress tracking, leaderboards, and collaborative challenges to promote peer-to-peer learning, healthy competition, and social interaction among students.

To ensure the effectiveness and relevance of the gamification platform, continuous evaluation and feedback mechanisms are integrated, allowing instructors to assess learning outcomes, identify areas for improvement, and iterate on content and activities accordingly. The platform's scalability and versatility enable seamless integration into existing educational frameworks, making it accessible to a diverse range of students and institutions seeking to enhance cybersecurity awareness and practices.

5. TECHNOLOGICAL BACKGROUND

The introduction section of this study serves the purpose of providing a comprehensive overview of the technological background related to platform development. It aims to establish a foundational understanding of key technological components, current trends, and emerging advancements shaping the domain. By delving into the hardware and software systems, as well as features provided and emerging technologies relevant to the field, this introduction sets the stage for a deeper exploration of how technology impacts various aspects of the development process, and how it influences decision-making, innovation, and societal dynamics.

5.1. Back-End Frameworks

The Back-end frameworks play a crucial role in modern web development, offering developers powerful tools and structures to build robust and efficient applications. Two prominent frameworks in this domain are Laravel and the .NET Framework.

Laravel, conceptualized by Taylor Otwell, stands out for its expressive syntax and adherence to the model-view-controller (MVC) pattern. Tailored for PHP-based web applications, Laravel simplifies common tasks like authentication, routing, sessions, and caching, enhancing the development of secure and scalable web solutions. Its user-friendly design and extensive feature set make it a preferred choice among PHP developers.

On the other hand, the .NET Framework, developed by Microsoft, provides a comprehensive platform for building diverse applications, including web, desktop, and mobile apps. Its core components like the Common Language Runtime (CLR) and Framework Class Library (FCL) streamline program execution and offer a rich set of functionalities for developers. With support for multiple programming languages and frameworks like ASP.NET for web applications and Windows Forms for desktop GUIs, the .NET Framework empowers developers to create versatile and high-performing applications.

In addition to these frameworks, Ruby on Rails (Ruby) and Expressive (PHP) contribute significantly to the back-end development landscape. Ruby on Rails, known for its convention-over-configuration approach and integrated testing framework, simplifies web application development and promotes code efficiency. PHP, part of the Laminas Project, adopts a middleware architecture that enhances application flexibility and modularity, making it an ideal choice for developers seeking customizable and efficient web solutions within the PHP ecosystem.

Overall, these back-end frameworks exemplify the evolution and diversity of tools available to developers, enabling them to create innovative and scalable applications that meet the demands of modern web development.

5.2. Front-End Frameworks

Front-end frameworks play a crucial role in shaping user experiences and interactions within web applications. In this exploration of potential frameworks, we delve into four key contenders:

Vue.js: Focuses on the view layer, employing a reactive and component-based structure for simplified web app development. It excels in project integration, data binding for UI synchronization, and offers transition effects and state management solutions for complex apps.

React.js: Widely used for dynamic UI creation, especially in single-page applications. Its component-based architecture and declarative approach streamline UI development, with seamless integration of libraries like Redux and React Router for enhanced functionality and performance.

Svelte: Innovatively shifts processing to compile-time, reducing boilerplate code and enhancing productivity. It ensures faster DOM updates and provides integrated features for animations and transitions, making it attractive for modern web development.

Ember.js: Adheres to the MVVM architecture, simplifying project development with standardized code structuring and integrated tools for managing application states and data. Powered by the Glimmer rendering engine, Ember.js ensures smooth UI updates for complex applications.

This comprehensive exploration of front-end frameworks offers valuable insights into their respective strengths and contributions, enriching the discourse on modern web development practices.

5.3. Databases

PostgreSQL, or Postgres, is a respected open-source object-relational database system known for its reliability, flexibility, and adherence to SQL standards. It has evolved since 1996 to handle various data types, advanced indexing, full-text search, and foreign data wrappers, making it suitable for diverse data workloads. ACID compliance ensures transaction integrity, and features like master-slave replication support scalability. PostgreSQL's extensibility with custom functions and compatibility with multiple programming languages enhance its adaptability across projects.

MySQL, another open-source RDBMS, uses SQL for database management. Developed by MySQL AB and later acquired by Sun Microsystems and Oracle Corporation, MySQL is known for its reliability, scalability, and speed. It's popular in web-based applications like WordPress, Facebook, and Twitter due to its ease of use, comprehensive documentation, and strong community support. MySQL serves as a foundational database solution across various projects, showcasing its versatility and dependability.

6. SYSTEM OVERVIEW

The main users of the system are students, MMU Administrator and System Administrator. All of them will access the system through the Internet as presented in Figure 1.

6.1. Student Functionalities

In our online learning platform, students have a range of features designed to enhance their experience and motivation:

- **Login**: Students can easily access the platform using their credentials.
- **Quizzes and Simulations**: They can engage with interactive quizzes and simulations to deepen their understanding.
- **Points and Rewards**: By completing activities and hitting milestones, students earn points and rewards like badges, encouraging active participation.
- **Progress Tracking**: Students can monitor their progress, check scores, view earned badges, and compare their performance with peers, fostering healthy competition.
- **Logout**: When done, students can securely log out from the platform.

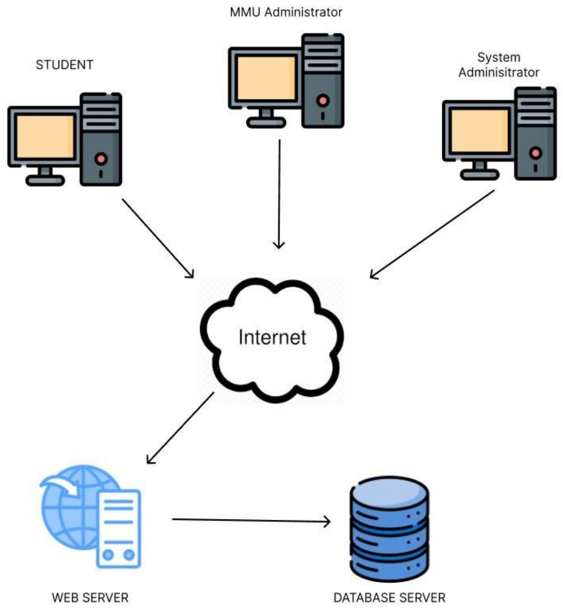


Figure 1. System Overview

6.2. MMU Administrator Functionalities

Our platform provides MMU administrators with essential tools to manage and enhance the learning experience:

- **Login**: Administrators can securely log in to the platform using their credentials.
- **User Account Management**: They have the capability to create, modify, or deactivate student accounts as needed, ensuring smooth account administration.
- **Progress Monitoring**: Administrators can access aggregated data on student performance, engagement, and participation to evaluate the platform's impact.
- **Content Customization**: MMU administrators can tailor and update platform content to align with MMU's cybersecurity curriculum and policies, ensuring relevance and accuracy.
- **Report Generation**: They can generate comprehensive reports on student participation, achievements, and overall platform usage, aiding in decision-making and assessment.
- **Logout**: Administrators can securely logout from the platform after completing their tasks.

6.3. System Administrator Functionalities

System administrators are pivotal in ensuring the smooth operation and security of our platform. Here are their key tasks:

- **Platform Maintenance**: They oversee the technical aspects, ensuring the platform's availability, security, and performance.
- **Updates and Maintenance**: System administrators apply software updates, patches, and security fixes to keep the platform up-to-date and secure.
- **User Role Management**: They manage user roles and permissions, assigning access levels to MMU administrators as needed for secure and authorized platform usage.
- **Technical Issue Handling**: System administrators troubleshoot and resolve technical issues promptly to maintain uninterrupted platform functionality.
- **Security Oversight**: They are responsible for ensuring platform security, including data protection measures and access control mechanisms.

7. SYSTEM ARCHITECTURE AND DESIGN

The cybersecurity awareness platform designed for MMU revolves around three key actors: MMU Administrators, System Administrators, and Students, each with defined roles and interactions within the system as presented in Figure 2. MMU Administrators are tasked with content curation and user engagement oversight, ensuring the platform's educational effectiveness. System Administrators focus on maintaining the technical infrastructure, guaranteeing system robustness and data security.

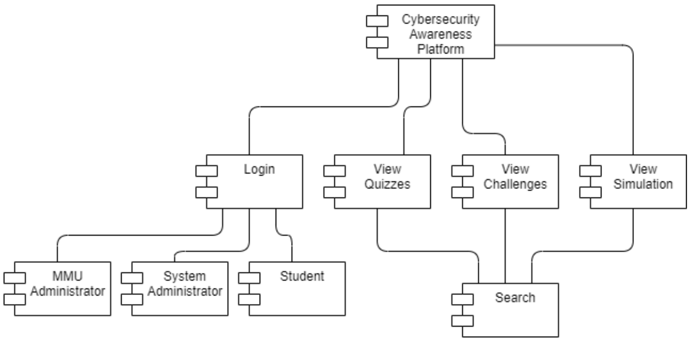


Figure 2. Overview of System Architecture

Students, the primary beneficiaries, access a range of interactive modules post-secure login, essential for personalization and user experience integrity. These modules include quizzes to assess cybersecurity comprehension, challenges for real-world problem-solving, and simulations for practical application in a controlled yet authentic context. Additionally, the platform facilitates efficient navigation and resource location through a search feature, empowering students to explore cybersecurity materials effectively. Subsequently, each segment of system architectures is presented as below.

7.1. System Architecture for Student Module

Figure 3 outlines the user interaction flow within the cybersecurity awareness platform designed for MMU students. It presents a step-by-step sequence of actions expected from student users as they navigate through the platform. Initially, students have options to access various educational resources such as quizzes, challenges, and simulations, which serve as primary channels for interactive learning about cybersecurity topics.

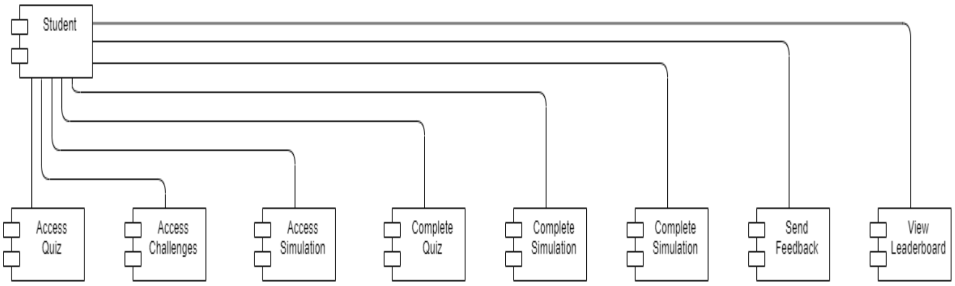


Figure 3. Overview of Student's Modules

Once engaged with these resources, students move on to complete quizzes and simulations, essential for evaluating their understanding and skills in cybersecurity. These activities contribute to their learning progress and may be monitored or assessed by the platform.

Further engagement is facilitated through the "Send Feedback" feature, allowing students to share their insights or questions about the platform, fostering a continuous feedback loop between students and platform administrators. Lastly, the "View Leaderboard" feature introduces a gamification element, enabling students to track their rankings based on performance in quizzes and simulations. This feature aims to motivate students by recognizing their achievements and fostering a competitive spirit, potentially enhancing their overall learning experience.

7.2. System Architecture for MMU Administrator Module

Figure 4 illustrates the administrative functionalities within a cybersecurity awareness platform tailored for MMU. It outlines the extensive responsibilities assigned to an MMU Administrator, including critical management and communication tasks crucial for platform operation and oversight.

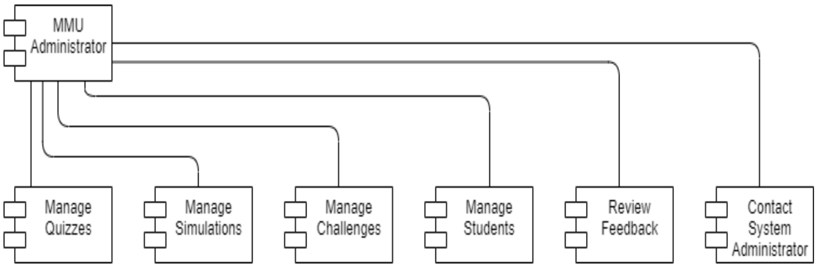


Figure 4. Overview of MMU Administrator Modules

The MMU Administrator possesses comprehensive management capabilities, overseeing quizzes, simulations, and challenges—key elements designed for interactive cybersecurity education. They also manage student profiles, monitoring progress, updating details, and handling enrolment or access permissions.

An essential aspect of the administrator's role is reviewing user feedback to ensure continuous improvement. The platform includes direct communication channels for collaboration with System Administrators, facilitating efficient issue resolution, system updates, and enhancements. In summary, the diagram presents a robust framework for MMU Administrators to effectively manage a cybersecurity platform, promoting interactivity and responsiveness to evolving cybersecurity challenges and educational methodologies.

7.3. System Architecture for System Administrator Module

The System Administrator within MMU's cybersecurity awareness platform holds pivotal responsibilities for ensuring system integrity and user satisfaction. This role encompasses tasks like managing user accounts, overseeing administrative roles, and maintaining adherence to security protocols as illustrated in Figure 5.

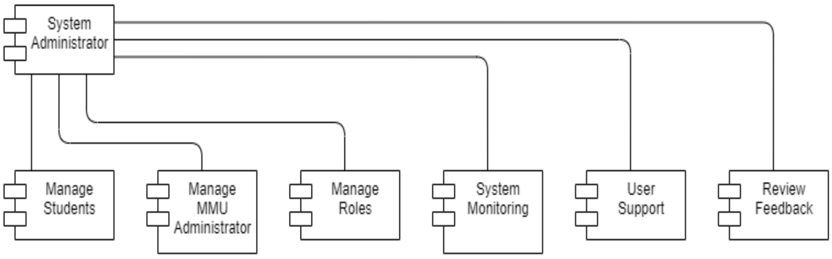


Figure 5. Overview of System Administrator Modules

System Administrators actively monitor the platform's performance, swiftly addressing any technical issues to uphold reliability. They also provide crucial user support, resolving queries promptly to enhance user experience. Incorporating user feedback is key, driving continuous improvements and aligning the platform with evolving user needs and technological advancements. Overall, the System Administrator plays a crucial role in maintaining system stability, enhancing user satisfaction, and driving innovation in cybersecurity education at MMU.

8. THE DATABASE CONNECTIVITY

The database schema depicted in Figure 6 illustrates the intricate structure of a gamified cybersecurity awareness platform meticulously crafted for the students at MMU. This platform is ingeniously designed to immerse MMU students in cybersecurity education through interactive engagements and incentivized learning experiences, culminating in a proactive cybersecurity culture within the university.

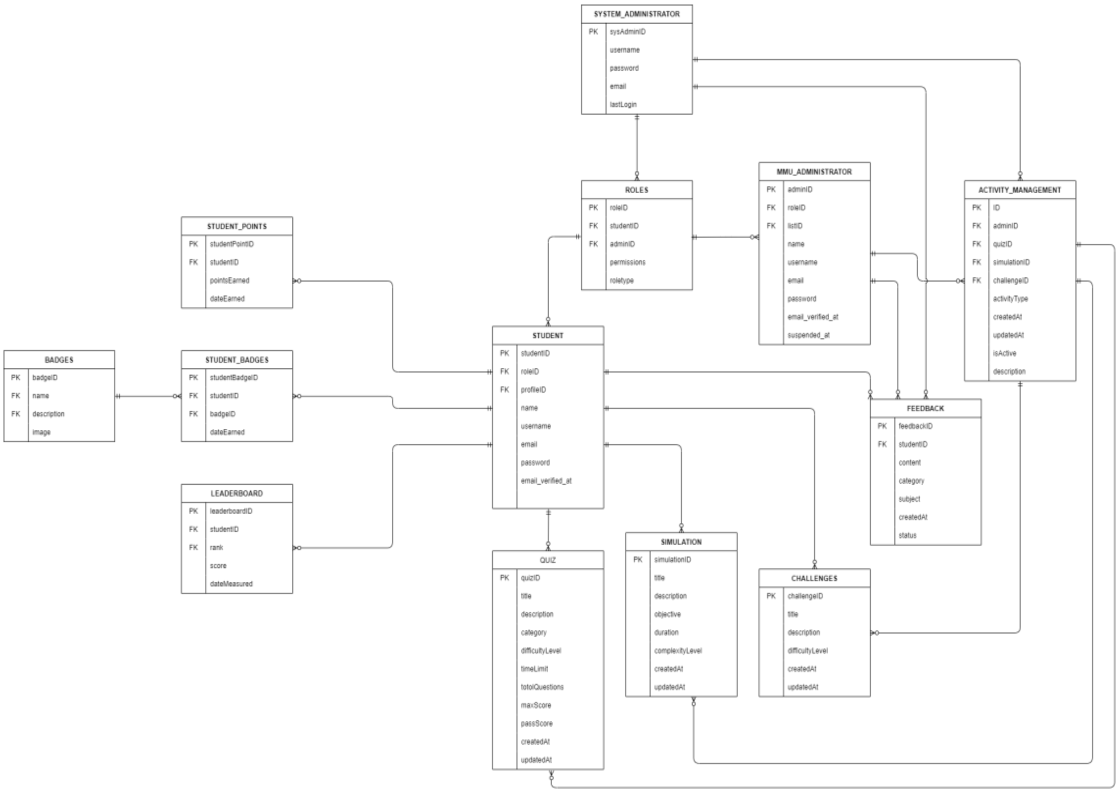


Figure 6. The Entity Relationship Diagram

At the core of this Entity-Relationship Diagram (ERD) lies the STUDENT table, meticulously architected to house detailed profiles of the primary users—the students. Within this table reside unique identifiers and pertinent personal details such as names, email addresses, and login credentials, ensuring meticulous tracking and management of each student's interactions with the platform.

Adjacent to the STUDENT table are the SYSTEM_ADMINISTRATOR and MMU_ADMINISTRATOR tables, strategically structured to administer users with administrative privileges. The SYSTEM_ADMINISTRATOR table encapsulates overarching system control, while the MMU_ADMINISTRATOR table focuses on administrative authority within specific university departments or functions.

The hierarchy of access rights within the platform is delineated in the ROLES table, delineating roles such as student participants, system overseers, and content administrators alongside their associated permissions. This role-based structure is pivotal in upholding the platform's integrity and security.

The gamification essence permeates through the ACTIVITY_MANAGEMENT table, meticulously chronicling a diverse spectrum of cybersecurity-related activities including quizzes, simulations, and challenges. These activities are further expounded upon in the QUIZ, SIMULATION, and CHALLENGES tables, encapsulating attributes such as titles, comprehensive descriptions, and metrics reflecting their complexity and educational merit.

Augmenting the gamification strategy are the STUDENT_POINTS and BADGES tables. The former tracks students' earned points from platform activities, while the latter catalogues an array of badges symbolizing students' accomplishments and educational milestones. The STUDENT_BADGES table acts as a pivotal nexus, associating students with their earned badges and providing a timestamped log of each achievement.

Crowning the gamified experience is the LEADERBOARD table, dynamically ranking students based on their accrued points and badges. This fosters a competitive and motivational milieu that spurs continual engagement and learning. In sum, the ERD epitomizes a robust and dynamic cybersecurity awareness platform tailored for MMU students, leveraging gamification to elevate educational outcomes and cultivate a proactive cybersecurity ethos within the university fabric.

9. DATA DICTIONARY FOR THE PROPOSED SYSTEM

The development and implementation of interactive learning platforms in cybersecurity education have become pivotal tools for fostering awareness and knowledge among students. This is especially true when considering the complexities of cybersecurity concepts and the dynamic nature of threats in today's digital landscape. In this context, a well-structured Data Dictionary (Table 2) plays a crucial role by providing a standardized reference point for terminology, definitions, and data structures within these interactive platforms. It ensures that stakeholders across the educational spectrum, from administrators to students, can effectively communicate, understand, and utilize the various elements and features of the platform, thereby enhancing the overall learning experience and cybersecurity awareness outcomes.

Table 2. Data Dictionary

Table	Field Name	Data Type	Data Format	Field Size	Description
STUDENT	studentID(PK)	bigint	NNNN	4	Unique identifier for each student
	roleID (FK)	bigint	NNNN	4	Foreign key to the role the student has
	name	varchar	-	50	Full name of the student
	username	varchar	-	100	Chosen username of the student
	email	varchar	-	150	Email address of the student
	password	varchar	Encrypted	255	Hashed password for the student's account
	email_verifie d_at	datetime	YYYYMM-DD HH:MM:SS		Timestamp when the email was verified
MMU_ADM INISTRATOR	adminID (PK)	bigint	NNNN	4	Unique identifier for each MMU administrator
	roleID (FK)	bigint	NNNN	4	Foreign key to the role the administrator has
	name	varchar	-	50	Full name of the MMU administrator
	username	varchar	-	100	Chosen username of the MMU administrator
	email	varchar	-	150	Email address of the MMU administrator
	password	varchar	Encrypted	255	Hashed password for the MMU administrator's account
	email_verified_ at	datetime	YYYY- MM-DD HH:MM:SS	-	Timestamp when the email was verified
	suspended_at	datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the account was suspended
SYSTEM_A DMINISTR ATOR	sysAdminID (PK)	bigint	Autoincrement	4	Unique identifier for each system administrator
	username	varchar	-	255	Chosen username of the system administrator
	password	varchar	Encrypted	255	Hashed password for the system administrator's account
	email	varchar	-	255	Email address of the system administrator

	lastLogin	datetime	YYYYMM-DD HH:MM:SS	-	Timestamp of the system administrator's last login
ROLES	roleID (PK)	bigint	Autoincrement	-	Unique identifier for each role
	studentID (FK)	bigint	-	-	Foreign key to the student associated with the role
	adminID (FK)	bigint	-	-	Foreign key to the administrator associated with the role
	permissions	Text	-	-	Specific permissions granted by the role
	roleType	Varchar	-	255	Name or type of the role
QUIZ	quizID (PK)	bigint	Autoincrement	-	Unique identifier for each quiz
	title	Varchar	-	255	Title of the quiz
	description	Text	-	-	Description of the quiz
	category	Varchar	-	255	Category of the quiz
	difficultyLevel	Varchar	-	255	Difficulty level of the quiz
	timeLimit	bigint	-	-	Time limit to complete the quiz in minutes
	totalQuestions	bigint	-	-	Total number of questions in the quiz
	maxScore	bigint	-	-	Maximum score achievable in the quiz
	passScore	bigint	-	-	Minimum score required to pass
	createdAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the quiz was created
	updatedAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the quiz was updated
SIMULATION	simulationID (PK)	bigint	Autoincrement	-	Unique identifier for each simulation
	title	Varchar	-	255	Title of the simulation
	description	Text	-	-	Description of the simulation
	objective	Text	-	-	Objective of the simulation
	duration	bigint	-	-	Duration of the simulation in minutes
	complexityLev el	Varchar	-	255	Complexity level of the simulation
	createdAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the simulation was created
	updatedAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the simulation was updated
CHALLENGES	challengeID (PK)	bigint	Autoincrement	-	Unique identifier for each challenge
	title	Varchar	-	255	Title of the challenge
	description	Text	-	-	Description of the challenge
	difficultyLevel	Varchar	-	255	Difficulty level of the challenge
	createdAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the challenge was created
	updatedAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the challenge was updated
ACTIVITY_ MANAGEMENT	activityID (PK)	bigint	Autoincrement	-	Unique identifier for each activity management entry
	sysAdminID (FK)	bigint	-	-	Foreign key to the system administrator responsible for the activity

	adminID (FK)	bigint	-	-	Foreign key to the MMU administrator responsible for the activity
	quizID (FK)	bigint	-	-	Foreign key to the related quiz
	simulationID (FK)	bigint	-	-	Foreign key to the related simulation
	challengeID (FK)	bigint	-	-	Foreign key to the related challenge
	activityType	Varchar	-	255	Type of activity (e.g., quiz, simulation, challenge)
	createdAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the activity was created
	updatedAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the activity was last updated
	isActive	Boolean	-	-	Indicates whether the activity is active or not
	description	Varchar	-	-	Description of the activity
FEEDBACK	feedbackID (PK)	bigint	Autoincrement	-	Unique identifier for each feedback entry
	studentID (FK)	bigint	-	-	Foreign key to the student who provided feedback
	content	Text	-	-	Actual textual content of the feedback
	category	Varchar	-	255	Category of the feedback (e.g., bug report, suggestion)
	subject	Varchar	-	255	Subject line or brief title of the feedback
	createdAt	Datetime	YYYYMM-DD HH:MM:SS	-	Timestamp when the feedback was submitted
	status	varchar	-	255	Current status of the feedback (e.g., new, reviewed, resolved)
BADGES	badgeID (PK)	bigint	-	-	Unique identifier for a badge
	name	Varchar	-	255	Name of the badge
	description	Text	-	-	Description of the badge
	image	Varchar	-	255	URL or path to the badge image
STUDENT_ BADGES	studentBadgeI D (PK)	bigint	-	-	Unique identifier for each badge assignment
	studentID (FK)	bigint	-	-	Foreign key to the student who earned the badge
	badgeID (FK)	bigint	-	-	Foreign key to the associated badge
	dateEarned	Datetime	YYYYMM-DD HH:MM:SS	-	Date when the badge was earned
STUDENT_ POINTS	studentPointID (PK)	bigint	-	-	Unique identifier for each point entry
	studentID (FK)	bigint	-	-	Foreign key to the student who earned points
	pointsEarned	bigint	-	-	Number of points earned
	dateEarned	Datetime	YYYYMM-DD HH:MM:SS	-	Date when the points were earned
LEADERBOARD	leaderboardID (PK)	bigint	-	-	Unique identifier for each leaderboard entry
	studentID (FK)	bigint	-	-	Foreign key to the student in the leaderboard
	rank	bigint	-	-	Rank of the student on the leaderboard
	score	bigint	-	-	Score of the student on the leaderboard

dateMeasured	Datetime	YYYYMM-DD HH:MM:SS	-	Date when the leaderboard was last updated

10. WIREFRAME AND INTERFACE DESIGNS

Upon logging into the application, users are greeted with the main page, serving as the gateway to a multifaceted learning experience. This interactive interface allows users to engage seamlessly by navigating through various sections via navigation buttons or accessing quizzes, challenges, and simulations, each offering distinct content and educational pathways. Figure 7 illustrates the wireframe of main page of the proposed platform.

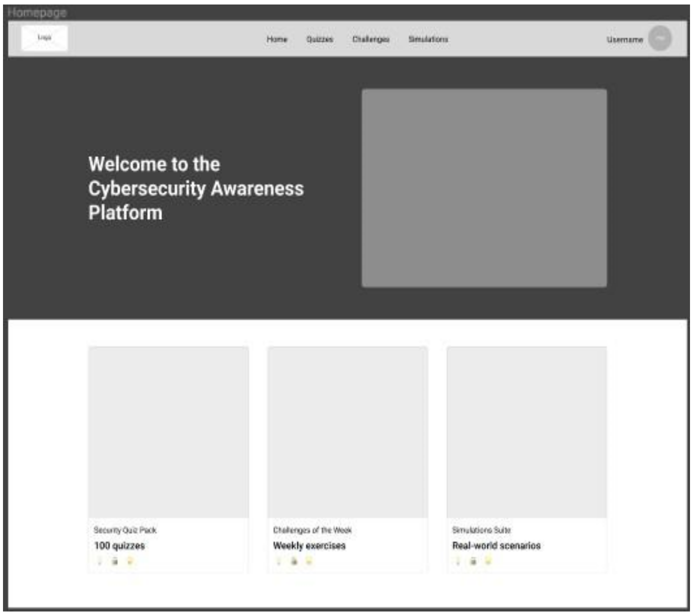


Figure 7. Wireframe – Home Page

The interface is strategically designed with a clear and informative header, providing users with intuitive options to explore the subject matter in-depth or initiate the quiz promptly. Central to the interface is a structured layout, meticulously divided to offer a comprehensive array of cybersecurity topics accompanied by concise yet informative descriptions. Additionally, the quiz section is seamlessly integrated into the interface, presenting users with a progressive sequence of questions designed to enhance their understanding and retention of key concepts as illustrates in Figure 8.

A notable feature of this interface is the results section situated at the bottom, aimed at providing users with immediate feedback on their quiz performance. This feedback mechanism not only enriches the learning experience but also facilitates continuous improvement and knowledge reinforcement. The design philosophy underlying this interface prioritizes navigational simplicity and educational efficacy, aligning seamlessly with the platform's core objective of fostering interactive learning experiences in cybersecurity.

Figure 9 illustrates the user-friendly webpage in which a search option and a clear "Start Simulation" button are added. It offers various "Simulated Scenarios" like "Phishing Attack" and "Malware Infection" with engagement metrics. New simulations are categorized by skill level. Users can give feedback through the "Simulation Feedback" form, promoting collaboration and improvement. This setup encourages active learning in cybersecurity.

The administrative dashboard is designed for efficient quiz management, ensuring user-friendly navigation and operational effectiveness as illustrated in Figure 10. Key features such as 'Dashboard,' 'Quizzes,' 'Challenges,' 'Simulations,' and 'Leaderboard' are organized in a sidebar for quick access. The main section focuses on quiz administration, allowing easy creation, editing, viewing, and deletion of quizzes. A graphical representation tracks the quiz creation trend over time, providing a visual insight into content development. Additionally, recent activities are monitored to gauge platform engagement. This dashboard layout optimizes administrative tasks and promotes data-driven decision-making for enhanced platform performance.

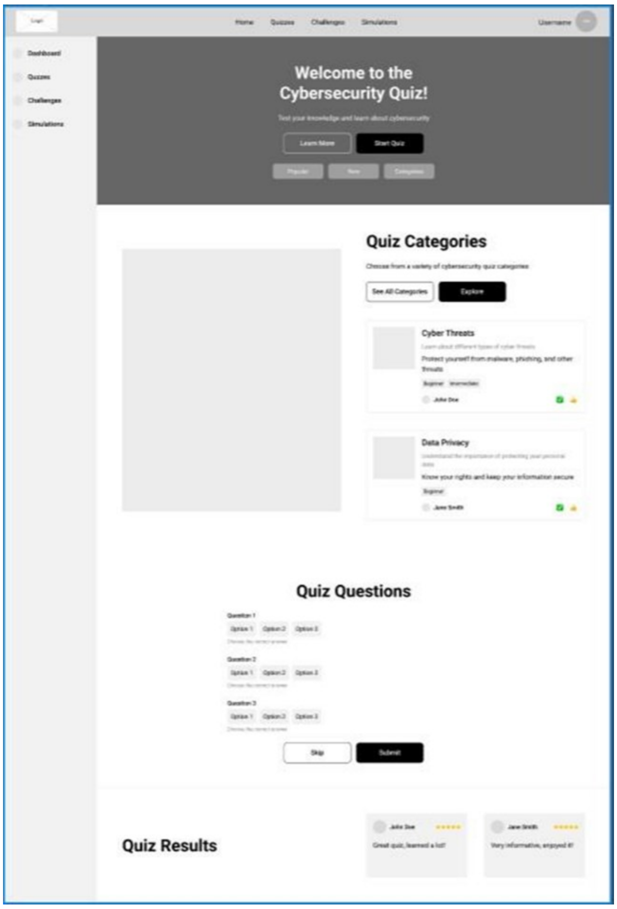

Logo
Home
Quizzes
Challenges
Simulations
Username
Dashboard
Quizzes
Challenges
Simulations
Welcome to the Cybersecurity Quiz!
Test your knowledge and learn about cybersecurity
Learn More
Start Quiz
Popular
New
Categories
Quiz Categories
Choose from a variety of cybersecurity quiz categories
See All Categories
Explore
Cyber Threats
Learn about different types of cyber threats
Protect yourself from malware, phishing, and other threats
Beginner
Intermediate
John Doe
Data Privacy
Understand the importance of protecting your personal data
Know your rights and keep your information secure
Beginner
Jane Smith
Quiz Questions
Question 1
Option 1
Option 2
Option 3
Choose the correct answer
Question 2
Option 1
Option 2
Option 3
Choose the correct answer
Question 3
Option 1
Option 2
Option 3
Choose the correct answer
Skip
Submit
Quiz Results
John Doe ★★★★★
Great quiz, learned a lot!
Jane Smith ★★★★★
Very informative, enjoyed it!

Figure 8. Wireframe – Quiz Page

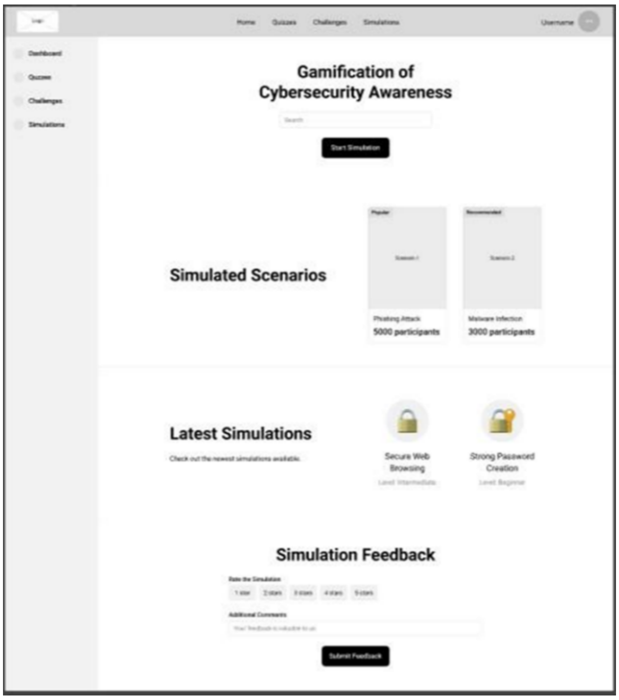
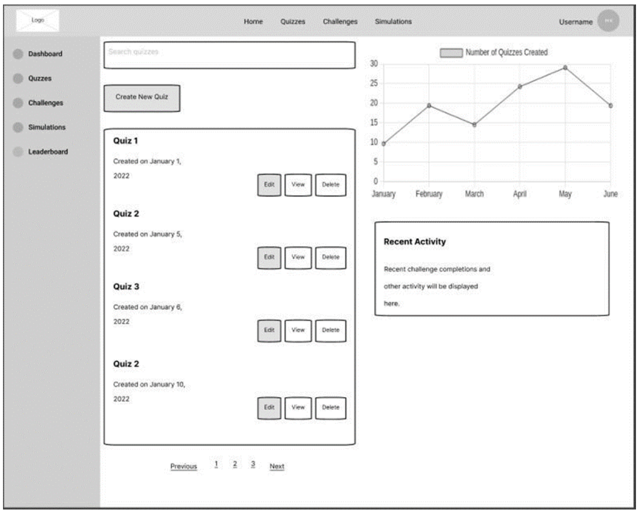


Figure 9. Simulation Web Page



Quiz 1

Created on January 1, 2022

Quiz 2

Created on January 5, 2022

Quiz 3

Created on January 6, 2022

Quiz 2

Created on January 10, 2022

Recent Activity

Recent challenge completions and other activity will be displayed here.

Figure 10. Quizzes Management Page – Administrator

11. ACHIVEMENT AND LIMITATION

Significant strides have been made in tailoring cybersecurity education to meet the unique needs of MMU students through the proposed cybersecurity education platform. By incorporating gamification strategies, the platform aims to enhance student engagement, creating a more enjoyable and effective learning atmosphere. Additionally, the platform's cost-effective design ensures broad accessibility, making it a viable option for educational institutions with limited budgets.

However, despite these advancements, several challenges persist within the proposed system that require attention. As the user base expands, scalability issues may arise, potentially impacting user experience and system performance. Moreover, the platform's reliance on specific technologies could hinder adaptability, posing challenges in keeping pace with evolving technological trends. This could also complicate the task of maintaining up-to-date and relevant instructional content to address the latest cyber threats effectively.

Furthermore, while the platform caters to MMU students, accommodating students from diverse linguistic and cultural backgrounds would necessitate further customization, a feature currently lacking in the system. Additionally, the absence of comprehensive analytics tools hinders the platform's ability to thoroughly assess student engagement and performance, limiting data-driven decision-making and advancements in educational strategies.

12. CONCLUSION AND FUTURE WORKS

The gamified cybersecurity education platform developed for MMU students marks a significant advancement in cybersecurity training tailored to diverse learning needs. This software effectively engages students and addresses financial constraints through personalized learning paths and interactive gamification, making it accessible to educational institutions. Future developments will focus on several key areas to further enhance the platform's effectiveness and reach:

- Scalability Enhancement - Implementing scalable infrastructure to accommodate a growing user base without compromising performance. Optimizing backend processes to handle increased traffic and data processing requirements.
- Technological Advancements - Incorporating cutting-edge technologies such as AI and machine learning for more advanced threat detection and mitigation. Introducing real-time threat simulations to provide hands-on experience in dealing with cybersecurity incidents.

- Advanced Analytics Integration - Introducing comprehensive analytics tools to track student engagement, progress, and performance in real-time. Utilizing data analytics to identify trends, patterns, and areas for improvement in cybersecurity training.
- Linguistic and Cultural Adaptation - Enhancing the platform's adaptability to accommodate students from diverse linguistic and cultural backgrounds. Offering content in multiple languages and culturally relevant scenarios to ensure inclusivity and effectiveness.
- Continued Focus on New Cybersecurity Issues - Regularly updating content and training modules to address emerging cybersecurity threats and challenges. Collaborating with industry experts and researchers to stay updated on the latest cybersecurity trends and best practices.

Through these future works, the gamified cybersecurity education platform will remain relevant, impactful, and highly effective in preparing students to tackle evolving cybersecurity issues.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable comments.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Adlil Khaliq bin Abdul Razack: Conceptualization, Data Curation, Investigation, Methodology, Validation,Writing – Original Draft Preparation;
Mohamad Firdaus bin Mat Saad: Project Administration, Supervision, Writing – Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. https://publicationethics.org/

No human or animal subjects were involved in this study, and no data collection was performed from social media platforms.

Given that human subjects were not involved, the requirement for informed consent was not applicable. Similarly, as no animal experiments were conducted, there was no need for ethical approval or animal licenses. Additionally, since data was not collected from social media platforms, considerations regarding participant consent and compliance with data redistribution policies of these platforms were not necessary.

We affirm that our research methods and practices fully comply with COPE guidelines, ensuring the highest standards of ethical integrity in our publication.

REFERENCES

[1] N. A. Savotina, E. I. Khachikyan, V. Bondarenko, and A. Ilyukhina, “Digital technology in modern education: Risks and resources,” *Journal of Physics: Conference Series*, IOP Publishing Ltd, 2020, doi: 10.1088/1742-6596/1691/1/012095.

[2] M. E. Erendor and M. Yildirim, “Cybersecurity Awareness in Online Education: A Case Study Analysis,” *IEEE Access*, vol. 10, pp. 52319–52335, 2022, doi: 10.1109/ACCESS.2022.3171829.

[3] CBS2 News Staff, “Idaho higher education institutions affected by worldwide data breach,” IdahoNews.

[4] T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, “Gamification of Cybersecurity for Workforce Development in Critical Infrastructure,” *IEEE Access*, vol. 10, pp. 112487–112501, 2022, doi: 10.1109/ACCESS.2022.3216711.

[5] A. Kamalulail, N. Ezzatul, N. A. Razak, S. Aisyhah Omar, Noreha, and M. Yusof, “Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus,” 2022. http://journale-academiauitmt.uitm.edu.mye

[6] R. Raju, N. H. A. Rahman, and A. Ahmad, “Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution,” *Asian Journal of University Education*, vol. 18, no. 3, pp. 756–766, Jul. 2022, doi: 10.24191/ajue.v18i3.18967.

[7] K. E. Rakow, R. J. Upsher, J. L. H. Foster, N. C. Byrom, and E. J. Dommett, “Student perspectives on their digital footprint in virtual learning environments,” *Front Educ (Lausanne)*, vol. 8, 2023, doi: 10.3389/feduc.2023.1208671.

[8] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Front Comput Sci*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[9] R. M. Abdulla, H. A. Faraj, C. O. Abdullah, A. H. Amin, and T. A. Rashid, “Analysis of Social Engineering Awareness Among Students and Lecturers,” *IEEE Access*, vol. 11, pp. 101098–101111, 2023, doi: 10.1109/ACCESS.2023.3311708.

[10] M. H. Alsulami *et al.*, “Measuring awareness of social engineering in the educational sector in the kingdom of saudi arabia,” *Information (Switzerland)*, vol. 12, no. 5, 2021, doi: 10.3390/info12050208.

[11] O. Fedor, “Internet Safety for College Students: The Ultimate Guide [2022].” https://www.findmysoft.com/cybersecurity/internet-safety-college-students/

[12] A. A. Owolabi, K. Okorie, N. Sola, and O. Sola, "Assessment of Cyber Ethics Behaviour among Undergraduate Students at the Nigerian Federal University of Agriculture and the University of Zululand in South Africa," Zambia Journal of Library & Information Science (ZAJLIS), vol. 6, no. 1, pp. 11-18, 2022. http://41.63.0.109/index.php/journal/article/view/73.

[13] M. Arogbodo, “Impacts of the Covid-19 Pandemic on Online Security Behavior within the UK Educational Industry,” 2022.

[14] Y. A. Najm, S. Alsamaraee, and A. A. Jalal, “Cloud computing security for e-learning during COVID-19 pandemic,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 3, pp. 1610–1618, Sep. 2022, doi: 10.11591/ijeecs.v27.i3.pp1610-1618.

[15] N. H. Al-Kumaim, A. K. Alhazmi, F. Mohammed, N. A. Gazem, M. S. Shabbir, and Y. Fazea, “Exploring the impact of the covid-19 pandemic on university students’ learning life: An integrated conceptual motivational model for sustainable and healthy online learning,” *Sustainability (Switzerland)*, vol. 13, no. 5, pp. 1–21, 2021, doi: 10.3390/su13052546.

[16] Cyberpatriot, “Cyberpatriot.” https://www.uscyberpatriot.org/

[17] Proofpoint, Inc. https://www.proofpoint.com/au

[18] Cisco Content Security User Group, “Cisco Security Awareness Program,” Cisco Public. https://www.cisco.com/c/dam/global/de_de/solutions/cisco-expert-talks/security-awareness.pdf

[19] J. C. Advisory, “2021 Trends show increased globalised threat of ransomware,” *TPL: White*, pp. 1–9, 2022.

[20] M. Aggarwal, “Ransomware Attack: An Evolving Targeted Threat,” *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, doi: 10.1109/ICCCNT56998.2023.10308249.

[21] F. Dahalan, N. Alias, and M. S. N. Shaharom, “Gamification and Game Based Learning for Vocational Education and Training: A Systematic Literature Review,” *Educ Inf Technol (Dordr)*, 2023, doi: 10.1007/s10639-022-11548-w.

[22] Z. A. Zainudin and N. Zulkiply, “Gamification in Learning: Students’ Motivation and Cognitive Engagement in Learning Business Using Quizizz,” *Asian Journal of University Education*, vol. 19, no. 4, pp. 823–833, 2023, doi: 10.24191/AJUE.V19I4.24928.

BIOGRAPHIES OF AUTHORS

I am **Adlil Khaliq bin Abdul Razack**, a Computer Science (Hons.) Cybersecurity student at MMU Cyberjaya. My research interests include network security, ethical hacking, and cryptography. My writing path began with my final year project, which focused on gamified cybersecurity awareness. I combine technical knowledge with narrative depth to investigate themes of privacy, security, and technology's societal implications. Outside of academia, I enjoy coding, gaming, and engaging in cybersecurity challenges, all of which stimulate my creative process.

Mohamad Firdaus bin Mat Saad is a Lecturer in Multimedia University. His research focuses on improving governance frameworks and project management methodologies, enhancing e-learning systems, and promoting effective technology adoption and information security practices. Ts. Firdaus is dedicated to fostering innovative solutions in his areas of specialization. With extensive expertise in these fields, he contributes significantly to advancing academic and practical knowledge in the specific field of study. Firdaus can be contacted via *firdaus.matsaad@mmu.edu.my*.