Journal of Engineering Research and Education
Volume 18, (Special Issue) 2026 [73-83]

Building Cyber Defense Skills: The CipherQuest Educational CTF Framework

Zainab S. Attarbashi[1], Muhammad Aliff Iman Abd Rasid[1], Muhammad Alif Haziq Mohd Razmi[1], Oula Sakka[2], and Azana Hafizah Mohd Aman[3]

[1]Department of Computer Science, Kulliyyah of Information & Communication Technology (KICT), International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Department of Information Systems, Kulliyyah of Information & Communication Technology (KICT), International Islamic University Malaysia, Kuala Lumpur, Malaysia
[3]Faculty of Information Science and Technology, Center for Cyber Security, Universiti Kebangsaan Malaysia, Bangi, Malaysia

ABSTRACT

As cyber threats grow increasingly sophisticated, equipping the next generation of cybersecurity professionals with practical, engaging training methods has never been more critical. Current cybersecurity education approaches face three key limitations: (1) traditional open-source CTF platforms often lack pedagogical alignment with academic curricula and lack institutional-grade user management and assessment tools, (2) game-based learning tools frequently sacrifice technical depth for accessibility, and (3) simulation environments may fail to foster competitive engagement crucial for skill retention. This paper evaluates three innovative approaches for cybersecurity education: Capture-the-Flag (CTF) competitions using the Ionian CTF model, which develops practical skills through challenge-based learning; CyberMoraba, an adaptation of the traditional African strategy game Morabaraba redesigned for cybersecurity instruction; and Cyberattack Simulator, offering realistic threat defense scenarios. Comparative analysis identified CTF as the most effective method for university students, combining technical skill development with competitive learning dynamics. Therefore, CipherQuest was developed, a CTF platform that synthesizes best practices from established systems (picoCTF, CryptoHack, HackTheBox) while incorporating IIUM curriculum-aligned challenges. The platform features jeopardy-style challenges across security domains with real-time feedback and progress tracking. Preliminary results show 90% of participants demonstrated improved cybersecurity knowledge and skills transferable to real-world scenarios. This research establishes that structured CTF platforms can effectively bridge theoretical cybersecurity education and practical application while maintaining academic consistency. The CipherQuest platform can provide universities with an evidence-based model for implementing engaging cybersecurity training that meets both educational objectives and industry needs.

Keywords: CipherQuest, Cyber Security Learning, Challenge-based Learning, Capture the Flag (CTF), CyberMoraba, CryptoHack

1. INTRODUCTION

In the rapidly evolving landscape of cybersecurity, despite the widespread availability of Capture the Flag (CTF) platforms [1], students encounter significant challenges in using these resources effectively. Existing CTF competitions often fail to provide comprehensive post-event educational materials, limiting opportunities for skill development[2]. The lack of detailed write-ups after competitions leaves participants without adequate guidance to analyze solutions or learn from their mistakes. Furthermore, the registration of dummy teams frequently overloads servers, causing technical disruptions and detracting from the experience of legitimate competitors. Additionally, the recurrence of similar challenges across events reduces problem diversity, constraining students' learning opportunities. These shortcomings underscore the need for an

*zainab_senan@iium.edu.my

improved CTF platform that addresses these issues while enhancing the educational value for cybersecurity students.

CipherQuest seeks to address these gaps by introducing an innovative CTF platform built for university students. Drawing on features from established competitions such as picoCTF[3], CryptoHack [4], and HackTheBox [5], CipherQuest offers structured, time-bound challenges designed to cultivate practical problem-solving and critical-thinking skills. Aligned with academic cybersecurity curricula, the platform incorporates real-time data analytics, predictive insights, and detailed challenge write-ups to create an immersive and pedagogically robust learning environment. By combining engagement with usability, CipherQuest enhances hands-on learning, equipping students with the competencies needed to thrive in the dynamic field of cybersecurity.

1.1 Ionian CTF

The Ionian CTF platform [6] serves as a cybersecurity learning environment that employs jeopardy-style Capture the Flag (CTF) challenges to enhance the knowledge and skills of undergraduate students in academic programs [7]. These challenges encompass different ranges of cybersecurity problems, enabling students to strengthen both their practical abilities and theoretical understanding of the field. The structured yet competitive framework of CTFs makes them an effective pedagogical tool, fostering student engagement and deeper comprehension of cybersecurity principles. By incorporating Ionian CTF into curricula, educators can offer a dynamic and structured approach to skill development, ensuring students acquire competencies essential for real-world applications.

The competitive aspect of CTFs encourages a stimulating learning environment, encouraging students to tackle complex security issues. Furthermore, this method bridges the gap between theoretical instruction and hands-on practice, equipping students with practical experience critical for future careers in cybersecurity. The Ionian CTF methodology incorporates two key elements to optimize learning:

1) Pre-engagement surveys: These assess participant preferences and skill levels, ensuring challenges are appropriately matched to their abilities. This adaptive approach maintains engagement by avoiding tasks that are either too difficult or too simplistic.
2) Storytelling components: By embedding challenges within narrative frameworks, the methodology enhances immersion and relatability. For instance, a CTF challenge might simulate a scenario where participants act as cybersecurity professionals investigating a fictional cyberattack on a corporate network. This narrative context provides meaningful motivation for technical tasks such as vulnerability identification, network traffic analysis, or malicious script decoding [7].

1.2 CyberMoraba

Morabaraba, also known as Umlabalaba, is a traditional two-player strategic board game originating from Africa [8], [9]. Predominantly popular among South Africa's Bantu-speaking communities, the game has been played for centuries and involves tactical piece movement and capture, requiring players to demonstrate strategic planning and decision-making skills. Its enduring appeal underscores both its cultural significance and its role in developing critical cognitive abilities (see figure 1).

The game is played on a distinctive board composed of three concentric squares connected by intersecting lines, forming 24 junction points [9], [10] as in figure 1. This unique geometric configuration creates a dynamic strategic space where players must carefully orchestrate their moves. Each player commands twelve pieces, traditionally represented by cowrie shells or stones, reinforcing the game's cultural authenticity. The board's design facilitates diverse tactical

possibilities, ensuring that each match presents a complex and intellectually stimulating challenge.

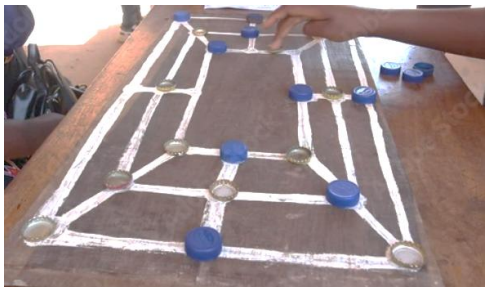

Figure 1. Morabaraba Game.

The core objective of Morabaraba is to form "mills"—specific linear arrangements of pieces—which grant the player the opportunity to capture an opponent's piece[8], [9]. Success demands foresight, adaptability, and strategic depth, as each move must balance offensive opportunities with defensive vulnerabilities. Unlike games of chance, Morabaraba is fundamentally a test of tactical proficiency, requiring players to anticipate and counter their opponent's strategies.

CyberMoraba is an innovative pedagogical tool that merges the traditional mechanics of Morabaraba with cybersecurity education. By using Morabaraba's inherent strategic framework, CyberMoraba provides an engaging platform for teaching cybersecurity principles. Players encounter simulated cybersecurity scenarios such as network defense, vulnerability identification, and attack mitigation, while adhering to the game's established rules and board structure. This fusion of traditional gameplay with modern cybersecurity concepts facilitates an interactive and culturally relevant learning experience.

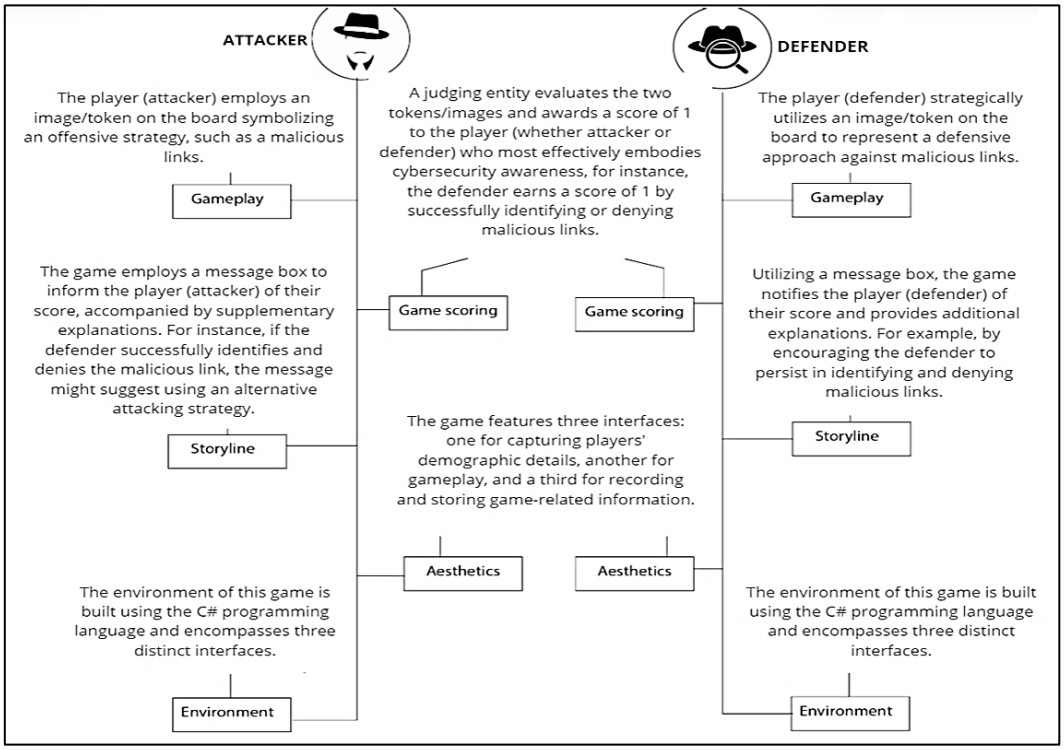

Figure 2. The CyberMoraba game components [8].

1.3 Cyberattack Simulator

The Cyberattack Simulator [11] adopts a novel pedagogical approach by enabling players to assume the role of an attacker, providing first-hand exposure to offensive cybersecurity techniques. This simulation framework facilitates practical engagement with real-world attack methodologies, including phishing campaigns, malware propagation, and social engineering strategies. Through interactive gameplay, participants can systematically explore various attack vectors, gaining experiential insight into how system and network vulnerabilities can be exploited.

The simulator employs a rigorously realistic representation of cyberattack scenarios [11]. This high-fidelity simulation enables participants to immerse themselves in environments that accurately replicate actual cyber threats. Such verisimilitude serves as a critical bridge between theoretical cybersecurity knowledge and practical competence, allowing learners to develop appropriate response strategies for genuine security incidents.

A key advantage of this approach is its capacity to generate valuable data on human decision-making under pressure. By confronting participants with authentic security dilemmas, such as evaluating suspicious links or managing resource allocation during a simulated breach, the simulator enables researchers to identify critical patterns. These include cognitive biases in security judgments, gaps in threat recognition, and deficiencies in operational protocols. Consequently, the platform serves not only as an educational tool but also as an empirical research instrument, contributing significantly to the understanding and improvement of organizational cybersecurity postures.

Table 2 Comparison of Some Cybersecurity Learning Systems

Platform Category	Core Educational Value	Ideal Audience	Key Strengths	Primary Limitations
Competitive Challenge Platforms (e.g., Capture-the-Flag (CTF), Hack The Box)	Learning through competitive problem-solving. Focuses on mastering specific skills via "Jeopardy-style" challenges and penetration testing labs in a scored, often ranked, environment.	University students, competitive learners, and professionals honing specific technical skills.	• Develops deep, practical expertise. • High engagement through leaderboards and flags. • Strong community and real-world tool usage.	Steep learning curve for beginners; can encourage "goal-oriented" rather than "foundational" learning.
Immersive Simulators & Ranges (e.g., CyberAttack Simulator, Cyber Range Platforms)	Understanding cyber warfare in a controlled, realistic environment. Ranges simulate entire corporate networks for team defense, while simulators often focus on the attacker's perspective.	Organizations, military teams, and advanced students training for enterprise-level incident response and attack analysis.	• Provides high-fidelity, real-world simulation. • Excellent for team-based exercises and understanding complex attack chains. • Prepares for large-scale operational threats.	Very high cost and complex setup; often overkill for individual skill development.
Gamified & Narrative Learning (e.g., CyberMoraba, Se rious Games)	Building engagement and conceptual knowledge through story and play. Uses	Beginners, non-technical staff, and students needing an	• Highly accessible and lowers the barrier to entry.	Limited hands-on technical practice; skills are often

	board game mechanics (CyberMoraba) or narrative-driven quests (CyberCIEGE) to teach strategic thinking and awareness.	engaging introduction to security concepts.	• Excellent for teaching strategy and awareness over technical execution. • Fosters cultural engagement (e.g., African board game adaptation).	conceptual rather than practical.
Structured & Adaptive Tutors (e.g., Cybersecurity Labs, AI-Powered Tutors)	Providing guided, personalized learning paths. Platforms like TryHackMe offer structured courses, while AI tutors provide adaptive, 24/7 guidance and theoretical instruction.	Beginners to intermediate learners seeking a self-paced, curriculum-driven approach to build foundational and intermediate skills.	• Lowers the initial learning barrier with step-by-step guidance. • Personalized pacing and content (AI Tutors). • Builds industry-aligned skills systematically.	Can lack the open-ended problem-solving of competitive platforms; AI tutors offer limited practical execution.

2. PROPOSED SYSTEM IMPLEMENTATION

CipherQuest was architected as an educational cybersecurity platform to address the pedagogical gap between theoretical security concepts and practical skill application within the Computer Science curriculum at the International Islamic University Malaysia (IIUM). Its core pedagogical mechanism is the implementation of Capture-the-Flag (CTF) challenges, designed to transform passive learners into active participants by engaging them in realistic, problem-based scenarios. This approach aims to enhance critical learning outcomes such as analytical reasoning, tool proficiency, and systematic vulnerability assessment. To ensure scalability, maintainability, and a clear separation of concerns, the platform's system architecture adheres to a structured three-tier model: The Presentation Layer provides the user interface, through which all user interactions occur, the Application Layer, or logic tier, contains the core platform functionality, processing requests and enforcing the business rules of the CTF challenges, and the Data Layer is responsible for the persistent storage of all information, including user accounts, challenge details, submissions, and scores.

This architectural choice directly supports CipherQuest's dual mission: to deliver a seamless and competitive challenge environment while integrating essential educational framework for guided learning. A comprehensive stakeholder analysis during the design phase identified three primary actors with distinct roles:

- Students: The primary beneficiaries who engage with challenges to develop their skills.
- Lecturers (Administrators): Who oversee courses, manage challenges, and monitor student progress.
- Developers: Responsible for the platform's upkeep and the creation of new challenges.

These actors interact through a suite of core functionalities, including secure authentication, a comprehensive challenge management system, tools for team coordination, and detailed progress tracking mechanisms, as illustrated in Figure 3.

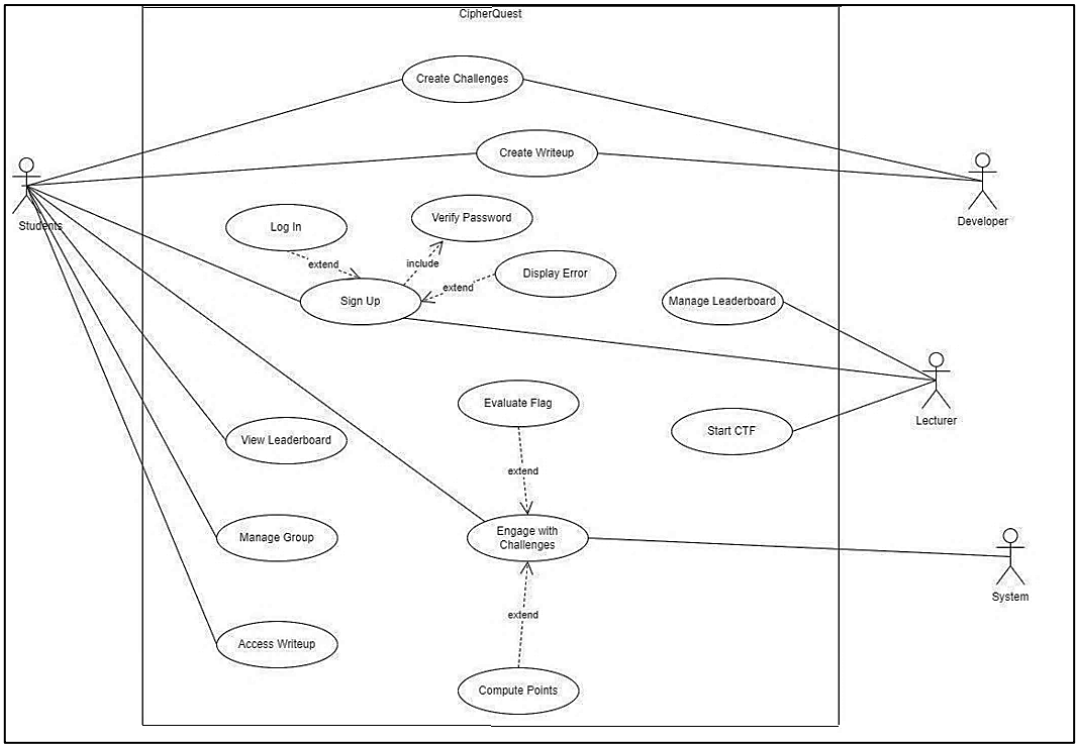

Figure 3. Primary Actors in CipherQuest Design.

The system's use cases were modelled to reflect authentic cybersecurity scenarios while aligning with the IIUM Cryptography course's learning outcomes as a start, since the system can be customized by the developers, it enables other courses to be added in the future. Table 3 summarizes CipherQuest's system requirements.

Table 3 System Requirements Specification

Requirement Type	Category	Description	Key Features/Criteria
Functional	User Authentication	Secure login and account management	•Registration/login system •Password encryption • Role-based access control
	Competition Setup	CTF competition creation and management	• Date/time configuration • Custom rule setting • Dynamic scoring system
	User Interaction	Challenge interface and progress tracking	• Challenge browser • Real-time flag validation • Personal dashboard
	Learning Resources	Educational content delivery	• Solution writeups • Curated references • Curriculum alignment
Non-Functional	Performance	System efficiency under load	•<500ms API response •Supports 500+ concurrent users • <1s leaderboard updates
	Security	Data and system protection	•OWASP compliance •Regular pentests • AES-256 encryption

	Usability	User experience quality	>90% task success rate •WCAG 2.1 compliant • Intuitive UI/UX

The implementation phase involved transforming the design into a fully operational system. The website was developed using *HTML*, *CSS*, and *JavaScript* for the frontend to create an intuitive and responsive user interface. Kali Linux was utilized as a development environment for ensuring secure and efficient implementation. The backend was configured to handle critical tasks such as data storage, submission evaluation, and scoring. Robust coding practices and iterative methods, such as debugging and functional validation, were adopted to address technical challenges and ensure smooth system functionality.

The platform's client-side was built as a dynamic single-page application using React.js, with the Material-UI library providing a modern, accessible interface that complies with WCAG 2.1 guidelines. The server-side architecture was developed with Node.js, implementing a secure and scalable backend to support the interactive frontend. The following table 4 details the core components and their specific implementations.

Database architecture utilizes *MySQL* with optimized indexes for frequent queries. The schema comprises five normalized tables (Users, Teams, Challenges, Submissions, Writeups) with *AES-256* encryption for sensitive fields. Relationships between entities follow strict referential integrity constraints, particularly for challenge-team-user associations. The platform's distinctive educational value emerges from its integration of competitive CTF elements with structured learning scaffolds. Real-time feedback mechanisms and curriculum mapping provide instructors with actionable insights into student competency development. The writeup feature shown in figure 4 provided educational support, making CipherQuest a distinctive platform compared to others.

Table 4 CipherQuest Platform Specifications

Layer	Component	Implementation	Purpose & Benefit
Frontend	Challenge Workspace	Embedded Terminal Emulator	Provides a realistic command-line interface directly in the browser, mirroring a professional penetration testing environment.
	Competition & Engagement	Real-time Leaderboard (WebSockets)	Fosters a competitive atmosphere with live score updates, enhancing user engagement and motivation.
	Documentation	Writeup Editor (Markdown Support)	Encourages students to document their problem-solving process, reinforcing learning through reflection and clear communication.
	Learning Support	Adaptive Hint System	Analyzes user attempt patterns to offer progressive, tailored guidance, providing pedagogical scaffolding.
Backend	Authentication & Authorization	JWT with Role-Based Access Control (RBAC)	Securely manages user sessions and permissions for students, lecturers, and administrators.
	Challenge Isolation	Docker Containerization	Creates safe, ephemeral environments for each challenge session, preventing cheating and system abuse.
	Data Integrity	Atomic Scoring Transactions	Ensures scoring events are processed completely and consistently, preventing point inaccuracies from race conditions.

	Flag Verification	SHA-256 Hashing	Securely validates submitted answers without storing the correct flags in plaintext.
	System Security	Rate-Limited API Endpoints (100 req/min)	Protects the system from abuse, brute-force attacks, and ensures fair resource allocation for all users.

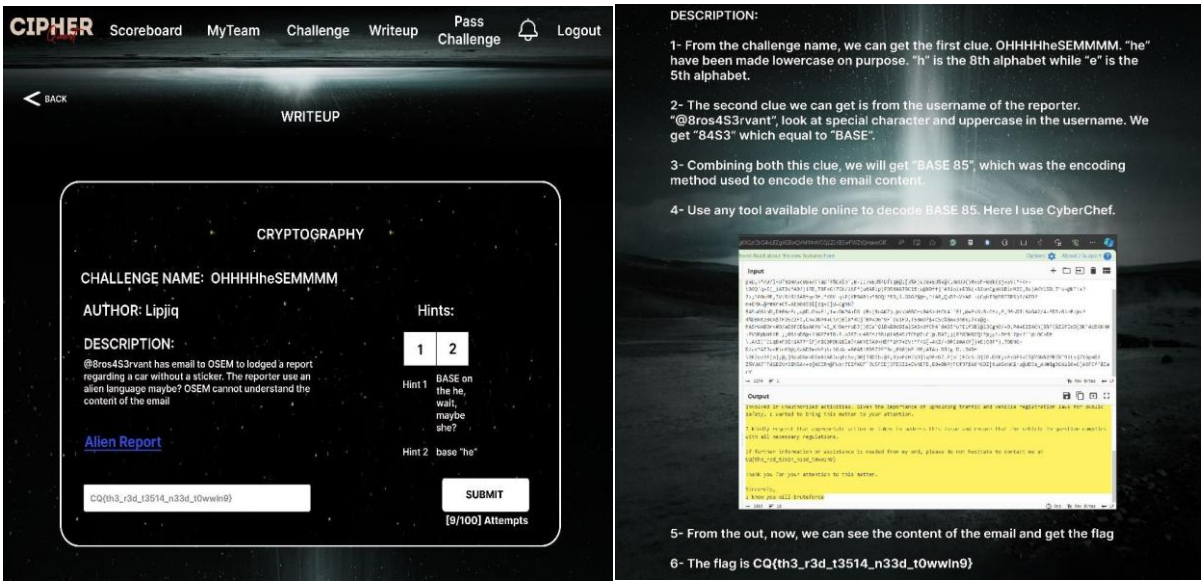

Figure 4. Write Up Page.

3. RESULTS AND DISCUSSION

The user feedback analysis yielded significant insights into the platform's efficacy and areas for improvement. As illustrated in Figures 5-8, the evaluation encompassed user demographics, platform usability, and pedagogical effectiveness.

The participant pool (n=10) demonstrated substantial prior exposure to cryptographic concepts, with 70% reporting formal or informal learning experiences (Figure 5). This baseline knowledge confirmed the sample's suitability for evaluating the platform's technical content. Regarding CTF experience, 40% of respondents had competition participation, while an additional 20% demonstrated awareness without direct involvement (Figure 6). This distribution reflects the platform's successful targeting of both novice and intermediate cybersecurity learners.

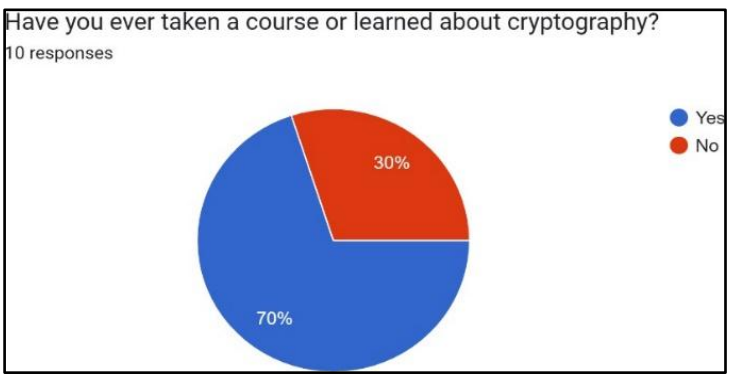

Figure 5. Have you ever taken a course or learned about cryptography?

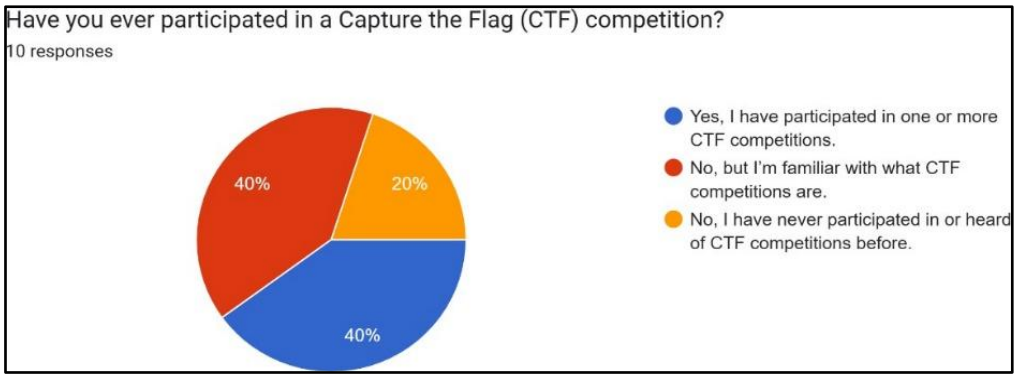

Figure 6. Have you ever participated in a Capture the Flag (CTF) competition?

Navigation efficiency emerged as a particular strength, with 80% of users rating the interface as "Very Easy" to navigate and the remaining 20% as "Easy" (Figure 6). Performance metrics were equally positive, with 90% of respondents reporting satisfactory loading times and system responsiveness (Figure 7). These results validate the architectural decisions implemented in the frontend development and system integration phases.

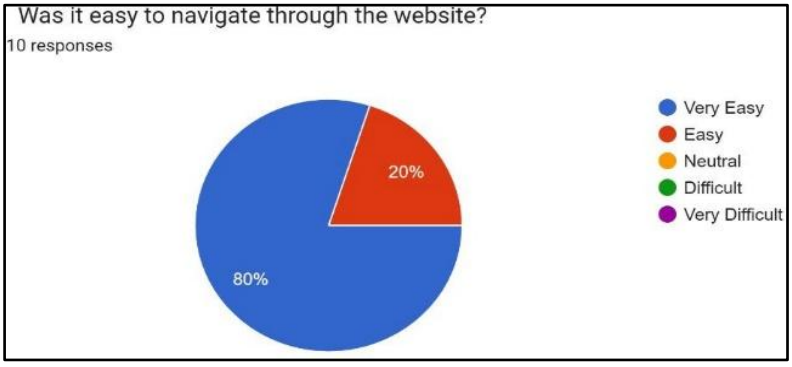

Figure 7. Was it easy to navigate through the website?

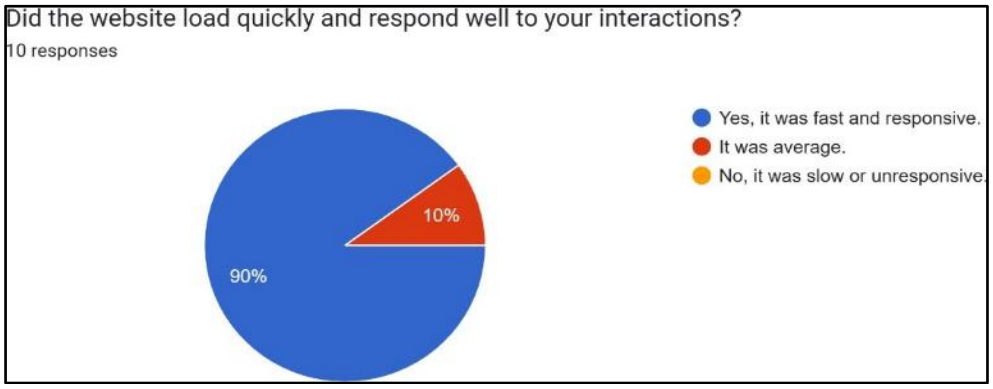

Figure 8. Did the website load quickly?

The difficulty calibration of cryptographic challenges showed appropriate variation, with 40% rating questions as "Just Right," while the remainder distributed across easier and more challenging perceptions (Figure 9). Most significantly, 90% of participants reported substantive learning outcomes, with 60% indicating substantial knowledge acquisition and 30% reporting moderate gains (Figure 10). These findings demonstrate the platform's success in translating CTF mechanics into effective learning experiences.

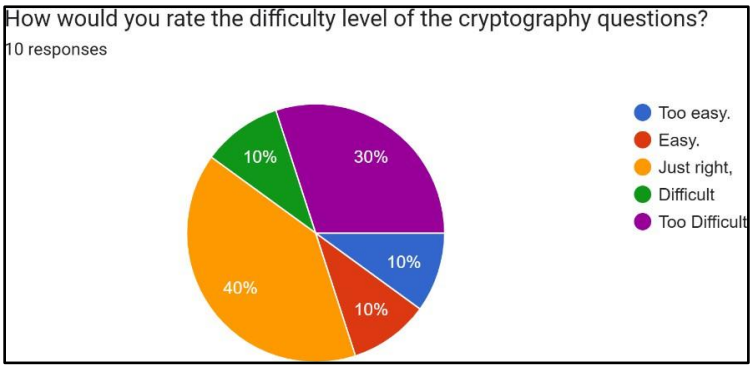

Figure 9. How would you rate the difficulty level of the cryptography questions?

Figure 10. Did cryptography questions help you learn or practice new concepts?

4. CONCLUSION AND FUTURE WORK

The development of CipherQuest followed a structured, iterative methodology encompassing design, implementation, and testing phases to create an effective cybersecurity education platform. During the design phase, careful consideration was given to system architecture, ensuring alignment with pedagogical objectives while prioritizing scalability, security, and usability. The implementation phase successfully transformed theoretical designs into a functional system, marked by key achievements such as the development of an automated scoring mechanism and the integration of a unique writeup feature, which facilitates reflective learning and distinguishes CipherQuest from existing CTF platforms. System testing confirmed the platform's reliability, usability, and performance, with evaluations demonstrating high user satisfaction in navigation, responsiveness, and educational value. The successful deployment of CipherQuest underscores its potential as a tool for cybersecurity education, effectively bridging theoretical knowledge and practical application through structured challenges and real-time feedback.

Future work will focus on expanding CipherQuest's capabilities to enhance both educational impact and user engagement. First, the platform's pedagogical framework will be strengthened through the introduction of structured learning paths, integrating guided tutorials with progressive challenges to benefit learners. Second, the challenge repository will be diversified to encompass additional cybersecurity domains, including network security, reverse engineering, and digital forensics, ensuring comprehensive skill development. Third, gamification elements—such as achievement badges, leaderboard tiers, and time-limited competitions—will be incorporated to sustain user motivation and encourage long-term participation. To improve

accessibility, a cross-platform mobile application will be developed, enabling users to engage with challenges beyond desktop environments. Furthermore, interactive tutorials will be introduced to lower the entry barrier for beginners, providing step-by-step guidance on fundamental concepts. Finally, the database infrastructure will be upgraded to a more robust system (e.g., PostgreSQL) to enhance scalability, optimize query performance, and ensure stability during peak usage. These enhancements will not only address current limitations but also position CipherQuest as a continually evolving platform capable of adapting to emerging trends in cybersecurity education.

REFERENCES

[1] S. J. Leudo, P. Braun, R. G. Sanfelice, and I. Shames, "A Hybrid Dynamical System Formulation of Capture-the-Flag Games," *IFAC-PapersOnLine*, vol. 58, no. 11, pp. 165–170, 2024, doi: 10.1016/j.ifacol.2024.07.442.

[2] T. Schafeitel-Tähtinen and W. Lazarov, "Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia," *Computer Applications in Engineering Education*, vol. 33, no. 5, Sep. 2025, doi: 10.1002/cae.70082.

[3] K. Zhang, S. Dong, G. Zhu, D. Corporon, T. McMullan, and S. Barrera, "picoCTF 2013 - Toaster Wars: When interactive storytelling game meets the largest computer security competition," in *2013 IEEE International Games Innovation Conference (IGIC)*, IEEE, Sep. 2013, pp. 293–299. doi: 10.1109/IGIC.2013.6659158.

[4] R. Beuran, "Capture the Flag Platforms," in *Cybersecurity Education and Training*, Singapore: Springer Nature Singapore, 2025, pp. 193–219. doi: 10.1007/978-981-96-0555-2_10.

[5] S. Kucek and M. Leitner, "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments," *Journal of Network and Computer Applications*, vol. 151, p. 102470, Feb. 2020, doi: 10.1016/j.jnca.2019.102470.

[6] S. Karagiannis and E. Magkos, "Adapting CTF challenges into virtual cybersecurity learning environments," *Information & Computer Security*, vol. 29, no. 1, pp. 105–132, May 2021, doi: 10.1108/ICS-04-2019-0050.

[7] S. Karagiannis and E. Magkos, "Adapting CTF challenges into virtual cybersecurity learning environments," *Information & Computer Security*, vol. 29, no. 1, pp. 105–132, May 2021, doi: 10.1108/ICS-04-2019-0050.

[8] M. Nkongolo, "Game Theory based Artificial Player for Morabaraba Game," in *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, IEEE, Jan. 2023, pp. 1210–1218. doi: 10.1109/ICSSIT55814.2023.10060972.

[9] N. Nkopodi and M. Mosimege, "Incorporating the indigenous game of morabaraba in the learning of mathematics," *S Afr J Educ*, vol. 29, no. 3, pp. 377–392, Aug. 2009, doi: 10.15700/saje.v29n3a273.

[10] M. Wa Nkongolo, "Infusing Morabaraba game design to develop a cybersecurity awareness game (CyberMoraba)," *International Conference on Cyber Warfare and Security*, vol. 19, no. 1, pp. 240–250, Mar. 2024, doi: 10.34190/iccws.19.1.1957.

[11] C. Scherb, L. B. Heitz, F. Grimberg, H. Grieder, and M. Maurer, "A Cyber Attack Simulation for Teaching Cybersecurity," 2023, pp. 129–116. doi: 10.29007/dkdw.