Darknet Duel

A Cybersecurity-Themed Card Game

Matthew Emmanuel O. Echavez
Cebu Institute of Technology - University
Cebu City, Philippines
matthewemmanuel.echavez@cit.edu

Brian Steve E. Pila
Cebu Institute of Technology - University
Cebu City, Philippines
briansteve.pila@cit.edu

Ephraim Jay A. Solasco
Cebu Institute of Technology - University
Cebu City, Philippines
ephraimjay.solasco@cit.edu

Kenjie B. Bentain
Cebu Institute of Technology - University
Cebu City, Philippines
kenjie.bentain@cit.edu

Scott Benzer Gitgano
Cebu Institute of Technology - University
Cebu City, Philippines
scottbenzer.gitgano@cit.edu

Eugene C. Busico
Cebu Institute of Technology - University
Cebu City, Philippines
eugene.busico@cit.edu

Abstract

Traditional cybersecurity education often fails to engage learners, leading to poor retention of critical concepts. To address this, we present *Darknet Duel*, a multiplayer web-based card game designed to gamify cybersecurity awareness. Built using a modern technology stack including React, Node.js, and Boardgame.io, the system ensures a responsive and scalable gaming experience. We conducted rigorous performance testing, demonstrating the server's ability to handle over 176 concurrent users. User evaluation involving 33 participants yielded a System Usability Scale (SUS) score of 50.9. While participants praised the game's concept and visual design, results indicate a need for improved onboarding to address the steep learning curve. This paper details the design, implementation, and evaluation of Darknet Duel, highlighting its potential as an engaging educational tool and outlining future improvements.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; *Social aspects of security and privacy*; • **Applied computing → Interactive learning environments**.

Keywords: Cybersecurity, Gamification, Card Game, Education, Awareness

1 Introduction

The increasing reliance on digital technologies has highlighted the importance of cybersecurity awareness. A significant section of the population is still unaware of the basic risks that the online world poses. Due to the fact that people make mistakes, fail to see potential dangers, and lack understanding of cybersecurity, people are often considered the weakest link in computer security and are therefore susceptible to cyberattacks.

Traditional learning resources are available, but they usually fail to maintain students' attention, which leads to inadequate understanding and recall of cybersecurity fundamentals. Students typically don't participate in traditional teaching techniques like lectures and textbooks, which results in poor material recall. Additionally, most of the gamified learning materials available today fall short of the goal because they are either too easy or too difficult, which keeps users from receiving a sufficient education.

To address this gap, we propose *Darknet Duel*, a gamified web-based card game designed to teach cybersecurity awareness in a strategic, engaging, and fun way. The game pits attackers against defenders, each using cards that represent ways of attacking, defending, and real-world cybersecurity events. By combining fast-paced gameplay with educational elements, Darknet Duel simplifies the concepts of cybersecurity while keeping users entertained.

2 Related Work

Gamification has emerged as a powerful strategy for enhancing cybersecurity awareness and education. This section reviews relevant literature on the effectiveness of gamification and analyzes existing solutions to identify gaps that Darknet Duel aims to address.

2.1 Gamification in Cybersecurity Education

Research consistently demonstrates the positive impact of gamification on engagement and knowledge retention. Institutions like the Berkeley Center for Long-Term Cybersecurity have highlighted the transformative potential of gamification in education [1]. Similarly, industry insights suggest that gamification is crucial for effective security awareness training, as it significantly boosts learner motivation [2].

Scholefield and Shepherd explored the use of gamification for password security education, developing an RPG for Android. Their findings indicated that participants enjoyed the interactive learning experience, suggesting that gamified

methods can effectively meet educational needs [3]. Studies on learning effectiveness further support this, showing that security awareness through gaming can lead to better educational outcomes [4].

Addressing the issue of knowledge deterioration, Fatokun et al. investigated gamification as an intervention strategy. Their study found that gamified learning opportunities could serve as a proactive measure to maintain high levels of user awareness and reinforce cybersecurity expertise, countering the tendency for knowledge to fade over time [5].

Williams et al. focused on students with no prior knowledge, using game mechanics to demystify difficult cybersecurity concepts. They discovered that elements like storytelling and puzzles not only raised interest but also improved comprehension and memory of the subject matter [6]. Similarly, Nwokeji et al. found that information systems students exposed to a gamified curriculum showed greater engagement and deeper understanding compared to those receiving standard instruction [7].

Furthermore, a systematic review by Gwenhure and Rahayu highlighted the effectiveness of gamification for non-IT professionals, a group often disengaged by conventional training. They concluded that gamification helps bridge the gap between technical material and non-technical audiences, fostering a security-conscious culture [8].

2.2 Existing Solutions

Despite the theoretical support for gamification, existing implementations often have limitations.

Byte Club Cybersecurity Card Game is a physical card-based game with a focus on cybersecurity education and strategic elements [9]. While it has an established brand and proven educational value, its physical nature limits its accessibility compared to a web-based platform. It is also not free to play, creating a cost barrier. Darknet Duel disrupts this by offering a web-based, multiplayer experience that is easily accessible.

Cyber Threat Defender is a multiplayer card game with collectible elements [10]. While effective, its reliance on deck-building and strategic depth similar to complex TCGs can present a steeper learning curve for casual players compared to Darknet Duel's streamlined mechanics.

Cyber Awareness Challenge focuses on education for government and military personnel [11]. However, it suffers from an outdated design and lack of interactivity, often relying on lengthy videos. Darknet Duel improves upon this by providing a modern, interactive, and engaging learning experience.

3 Methodology

3.1 System Architecture

Darknet Duel is built as a modern web application using a robust technology stack designed for performance, scalability, and user experience.

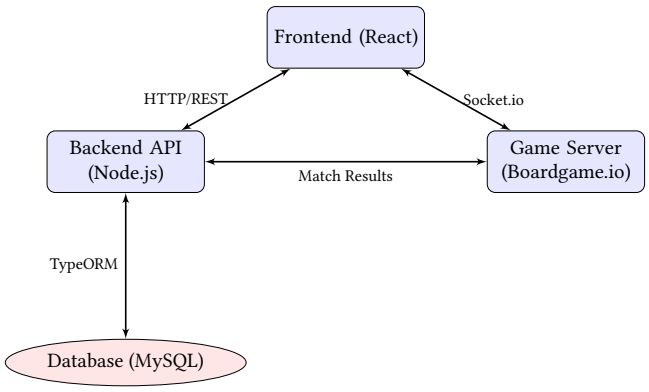

Figure 1. High-Level System Architecture

3.1.1 Frontend. The user interface is built using React, a popular JavaScript library for building user interfaces. We utilize Vite as the build tool for its fast development server and optimized production builds. For styling, we employ TailwindCSS and DaisyUI to create a modern, responsive, and visually appealing design that enhances the gaming experience.

3.1.2 Backend API. The backend API is developed using Node.js and Express, providing a flexible and scalable server environment. We use TypeScript to ensure type safety and code maintainability. Data persistence is managed by MySQL, with TypeORM serving as the Object-Relational Mapper (ORM) to interact with the database efficiently. Authentication is handled via server-side sessions, which allows for granular control over user access, including the ability to invalidate sessions for logging out or banning users.

3.1.3 Game Server. To manage the real-time multiplayer state, we utilize Boardgame.io. This framework simplifies the development of turn-based games by handling state management, move validation, and synchronization between clients. Communication between the client and the game server is facilitated by Socket.io, ensuring low-latency updates during gameplay.

3.2 Justification

The choice of React allows for a dynamic and responsive UI, essential for a card game. Node.js and Express provide a lightweight yet powerful backend capable of handling concurrent requests. Boardgame.io was selected specifically for its specialized features for turn-based games, reducing the

complexity of implementing game logic and state synchronization from scratch.

4 Implementation

4.1 Development Model

We adopted the Waterfall Model for the development of Darknet Duel. This structured approach allowed us to have a stable development lifecycle, ensuring that each phase—from requirements gathering to design, implementation, and testing—was completed before moving to the next. This was particularly beneficial for defining the game rules and mechanics clearly before writing code.

4.2 Deployment and DevOps

To ensure consistent environments and ease of deployment, we utilized Docker to containerize both the frontend and backend applications. This eliminates "it works on my machine" issues and simplifies dependency management.

For Continuous Integration and Continuous Deployment (CI/CD), we implemented GitHub Actions. This automated pipeline runs tests and builds the Docker images whenever changes are pushed to the repository, ensuring code quality and rapid feedback.

The application is deployed on a DigitalOcean server (Droplet). The Docker containers are orchestrated to run the web server, API server, and database on the cloud infrastructure, making the game accessible to users over the internet.

5 Performance Testing

Before deploying the application, we conducted rigorous performance testing to evaluate the server's capacity and stability under load.

5.1 Test Environment

The server environment consisted of a quad-core AMD Ryzen 3 5300U processor with 20GB of RAM, running Ubuntu Server. This setup was chosen to simulate a realistic hosting environment for a medium-scale web application.

5.2 Methodology

We developed a custom Node.js script to simulate multiple users performing concurrent API calls. Each simulated user executed seven specific API calls simultaneously, representing the most common actions a real user would perform:

- **Lobby:** Browsing the lobby list and creating a new lobby.
- **Login:** Authenticating with the server.
- **Profile:** Retrieving user profile data.
- **Register:** Creating a new user account.
- **Search:** Searching for other users.
- **Socket:** Initiating a game session and simulating moves.
- **Update:** Updating profile information.

The test started with a single user and incrementally added $n + 1$ users. The script was designed to automatically halt if any endpoint failed to respond within a maximum tolerable threshold of 5000ms.

5.3 Results

The stress test successfully handled a load of 176 concurrent users. The latency remained within acceptable limits until the 177th user was added, at which point a random ping spike on an API endpoint caused the response time to exceed the 5000ms threshold, halting the script.

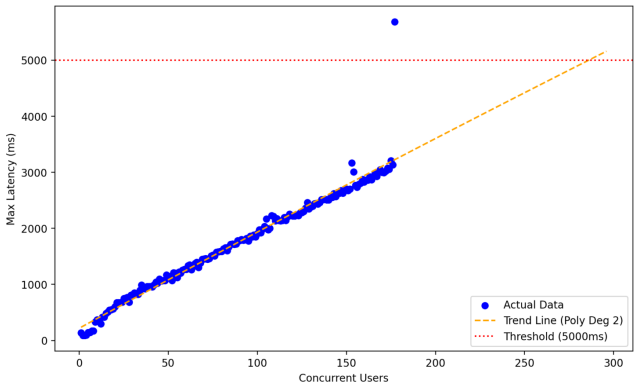

Figure 2. Maximum Concurrent Users

Extrapolating from the data collected, the server could theoretically handle up to 286 concurrent users before reaching critical failure points, assuming ideal conditions.

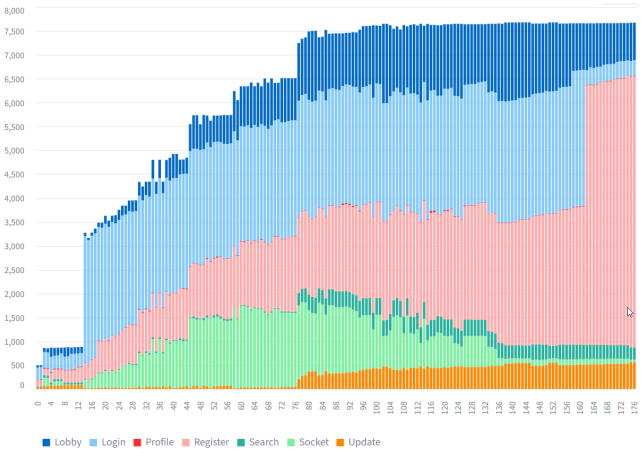

Figure 3. Latency Breakdown by Endpoint

Analysis of the 177th run revealed that the **Register** endpoint experienced the highest latency. This is consistent with expectations, as registration involves a write operation to the database, which is inherently more resource-intensive than read operations.

It is important to note that this test assumes a "worst-case" scenario where every user is placing maximum load on the server simultaneously. In a real-world scenario, user activity would likely be more distributed, suggesting that the server could theoretically handle a higher number of active users than the stress test indicates.

6 Results and Evaluation

To evaluate the usability and effectiveness of Darknet Duel, we conducted a System Usability Scale (SUS) test with 33 college student respondents within Cebu Institute of Technology - University within a one-day period.

6.1 SUS Results

The average SUS score calculated from the participant responses is 50.9. According to standard SUS interpretation, this score falls into the "Marginal" or "Low" acceptability range. While some users found the system easy to use and integrated well, others reported challenges with complexity and learning the game mechanics.

6.2 Qualitative Feedback

We also collected open-ended feedback to understand user sentiments better. Participants praised the User Interface (UI) and the concept of the game. Many found the idea of learning cybersecurity through a card game to be "fun," "unique," and "educational." The visual design and animations were also highlighted as positive aspects.

However, the primary challenge reported by users was the complexity of the game mechanics and the steep learning curve. Several users mentioned that the tutorial had bugs or was not sufficient to fully understand the game. A specific issue was raised regarding pop-up cards blocking the view of important details during the tutorial and gameplay.

To address these issues, users suggested improving the tutorial to be more comprehensive and bug-free. Visual cues, such as clearer indicators for whose turn it is and better highlighting of interactive elements, were also requested. Some users expressed a desire for a "practice mode" against an AI opponent before playing against real people.

7 Conclusion

Darknet Duel represents a significant step towards making cybersecurity education more accessible and engaging. By gamifying complex concepts, we have created a platform that appeals to a broad audience.

While the initial evaluation shows promise in terms of concept and design, the SUS score of 50.9 indicates that there is significant room for improvement in terms of usability and learnability. The feedback highlights the need for a more robust tutorial and a simplified onboarding process.

Moving forward, we plan to address these issues by refining the game mechanics, fixing the reported bugs in the tutorial, and enhancing the visual feedback system. We believe that with these improvements, Darknet Duel can become a highly effective tool for raising cybersecurity awareness.

Acknowledgments

We would like to thank our test participants for their valuable feedback.

References

[1] Berkeley Center for Long-Term Cybersecurity. *Gamification of Cybersecurity Education*. Retrieved from https://cltc.berkeley.edu/publication/gamification-of-cybersecurity-education

[2] Inspired eLearning. *The Importance of Gamification in Security Awareness Training*. Retrieved from https://inspiredelearning.com/blog/gamification-importance-security-awareness-training

[3] Scholefield, S., & Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. *SpringerLink*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-22351-9_13

[4] International Journal of Cybersecurity Intelligence & Cybercrime. *Security Awareness Through Gaming: A Study on Learning Effectiveness*. Retrieved from https://sites.asee.org/se/wp-content/uploads/sites/56/2021/01/2020ASEESE117.pdf

[5] Faith Fatokun, Zalizah Awang, Suraya Hamid, Johnson O. Fatokun, & Azah Norman. (2024). Cybersecurity knowledge deterioration and the role of gamification intervention. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 43(1), 66–94. https://doi.org/10.37934/araset.43.1.6694

[6] Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. (2024). Leveraging gamification and game-based learning in Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education*, 11(1), 8. https://doi.org/10.53735/cisse.v11i1.186

[7] Nwokeji, J. C., Matovu, R., & Rawal, B. (2020). The Use of Gamification to Teach Cybersecurity Awareness in Information Systems. Retrieved from https://www.researchgate.net/publication/349917575

[8] Gwenhure, A. K., & Sapty Rahayu, F. (2024). Gamification of cybersecurity awareness for Non-IT Professionals: A Systematic Literature Review. *International Journal of Serious Games*, 11(1), 83–99. https://doi.org/10.17083/ijsg.v11i1.719

[9] CyberSec Games. *Byte Club Cybersecurity Card Game*. Retrieved from https://www.cybersecgames.com

[10] Center for Infrastructure Assurance and Security (CIAS). *Cyber Threat Defender*. Retrieved from https://cias.utsa.edu/ctd/

[11] Department of Defense Cyber Exchange. *Cyber Awareness Challenge*. Retrieved from https://public.cyber.mil/training/cyber-awareness-challenge/