IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, December 2025
Impact Factor: 7.67

CipherQuest: A Cybersecurity Puzzle Game

Mrs. Bhagyashali Jadhav, Keisha Rai, Janhavi Taware, Tanvi Patil, Anjali Rathod
Department of Computer Engineering
Pimpri Chinchwad Polytecnic Pune, India
bhagyashalijadhav@gmail.com , Keisharai07@gmail.com, janhavitaware15@gmail.com,
tanvip1117@gmail.com, rathodanjali868@gmail.com

Abstract: *Traditional cybersecurity training is often outdated and doesn't prepare users for the complex nature of today's digital threats. This paper presents CipherQuest, an interactive puzzle game that aims to turn complicated security concepts into an engaging learning experience. The project includes a unique Threat Persona Engine (TPE) that uses adaptive AI to mimic various attacker behaviors, including the "Phishlor" and "CipherShade". By leading the main character, Nova, through three levels of digital challenges, players get hands-on experience in spotting phishing attempts, defending against social engineering, and using technical safeguards like two-factor authentication. The results indicate that this game-based, scenario-driven approach significantly boosts user engagement and helps with knowledge retention compared to traditional methods.*

Keywords: CipherQuest, Cybersecurity Awareness, Gamification, Threat Persona Engine, Adaptive Learning, Phishing Defense, Serious Games

I. INTRODUCTION

In today's digital age, the human factor is the weakest link in the security chain. Most data breaches happen not due to software failures, but because of human mistakes, like clicking on harmful links or using weak passwords. Traditional training, with its long videos and heavy text, often seems dull and ineffective[1].

CipherQuest aims to change this. It is an immersive puzzle game where players take on the role of Nova, a teenage girl exploring a digital world filled with hidden dangers. The game shifts away from passive learning by forcing players to make active defensive decisions, allowing them to build "digital armor" through hands-on gameplay[1].

CipherQuest not only teaches defense but also addresses the psychological side of cybercrime with its story-driven approach. By placing players in Nova's life, the game creates an emotional connection that makes the stakes feel personal instead of theoretical. This immersion is key because it reflects the intense environment of real attacks, where panic can lead to bad choices[2].

As players repeatedly interact with various threat scenarios, they don't just memorize rules; they develop quick instinctive "cyber-reflexes". As a result, the game acts as a link between awareness and action, ensuring that when users face a real Phishlor or social engineer, they have the confidence and clarity to respond effectively[2].

1.1 Background

Contemporary adversaries employ sophisticated maneuvers, such as psychological manipulation and deceptive communication. Conventional training programs frequently lack hands-on engagement with these specific tactics; consequently, individuals often remain at risk despite possessing theoretical expertise. This initiative focuses on developing an immersive framework that requires participants to navigate critical decision-making paths to advance[1].

A primary challenge in typical security education is the "knowledge-action disconnect". While users may grasp security protocols conceptually, they often falter when applying them to practical, real-world scenarios. CipherQuest addresses this discrepancy by integrating educational content into a high-pressure narrative. In this environment, the protagonist, Nova, encounters immediate repercussions based on the player's choices, bridging the gap between theory and practice.

DOI: 10.48175/IJARSCT-30658

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, December 2025 Impact Factor: 7.67

1.2 Contribution of this Work

CipherQuest introduces several distinct innovations designed to modernize the way cybersecurity is taught, moving away from generic advice toward a personalized, high-engagement framework:

• Threat Persona Engine (TPE): At the heart of the game is the TPE, system that goes beyond static, predictable obstacles. It features different attacker types, ranging from the reckless "Script Kiddie" to the highly manipulative "Social Engineer", each with a unique set of tactics. By simulating these specific behaviors, the game prepares players for the various "personalities" of cybercrime they may encounter in reality.

• Adaptive Intelligence: Unlike traditional modules that have a fixed difficulty level, CipherQuest has a dynamic adjustment system. The engine constantly monitors player metrics, such as reaction time, accuracy in identifying threats, and frequency of errors. If a player is easily handling challenges, the AI increases the complexity of the attacks. Conversely, if a player struggles, the system adjusts to provide a supportive learning experience.

• Behavioral Reinforcement: The integration of Pixi, a "Duolingo-style" companion mascot, creates a key psychological link between theory and practice. Pixi provides more than just answers; she offers real-time, context-aware feedback and encouragement. This immediate reinforcement helps players develop safe digital habits, such as checking for URL discrepancies or enabling 2FA, by turning these actions into instinctive "cyber- reflexes". By providing positive feedback during stressful simulated breaches, the game effectively turns temporary awareness into lasting behavioral change. Breaches, the game successfully converts temporary awareness into long-term behavioral change.

II. PROPOSED METHODOLOGY

The CipherQuest architecture is designed to create a seamless transition from theoretical awareness to practical application. Below is an elaboration on each core component of the system:

2.1 System Architecture

The CipherQuest ecosystem is powered by four synchronized pillars designed to foster a bespoke and immersive educational journey:

- Virtual Interaction Layer: Rather than utilizing a series of linear screens, this module leverages robust development tools to construct a responsive, level-based universe. Players navigate the digital landscape as the character Nova, interacting with simulated touchpoints ranging from administrative terminals to personal social media interfaces. This high-fidelity replication ensures that the behavioral changes learned in-game translate effectively to real-world cyber hygiene.
- Adversarial Behavior Core (TPE): The Threat Persona Engine functions as the tactical "intellect" behind the game's opponents. It transcends basic automation by employing three specific profiles that adjust to the player's proficiency:
  Tier 1 (Script Kiddie): Focuses on entry-level, automated threats that escalate as the user masters basic defenses.
  Tier 2 (The Social Engineer): Centers on human-centric vulnerabilities, utilizing deceptive narratives and psychological bait to test the user's skepticism.
  Tier 3 (APT - Advanced Persistent Threat): Simulates complex, long-term incursions that require strategic, multi-step countermeasures. These entities analyze player habits to provide a truly individualized challenge.
- Integrated Guidance (Pixi): To prevent player frustration, the system incorporates Pixi, a mascot that serves as a pedagogical mentor. Pixi monitors performance in real-time to offer contextual suggestions, encouragement, and customized pathing. This interactive support system bridges the gap between challenging content and user capability, reinforcing safe habits through positive reinforcement.
- Analytical Logic Engine: Serving as the backend "judge", this component quantifies every player action. It operates a real-time consequence model where security failures result in the loss of one of three "lives". This creates a high-stakes psychological environment, prompting users to critically analyze their mistakes. To

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, December 2025
Impact Factor: 7.67

underscore the gravity of security lapses, a mandatory cooldown period occurs if all lives are lost, allowing the user to reflect before attempting the module again.

2.2 Workflow

- Deployment Phase: Users initiate their journey at Stage 1, "The Phishing Pond". This entry point establishes the baseline for evaluating the player's reactive capabilities against incoming threats.
- Event Triggering: The system activates specific threat scenarios, such as high- urgency deceptive alerts (e.g."urgent prize notifications"),which demand immediate cognitive assessment and response.
- Defensive Intervention: Participants utilize interactive mechanics to neutralize threats. This includes isolating fraudulent communications through drag-and-drop actions or executing software patches via swipe gestures to resolve vulnerabilities.
- Validation & Reward: Upon successful mitigation of all Stage 1 scenarios, users are granted the "Cyber Guardian" credential alongside an official, exportable Cyber Safety Certification.

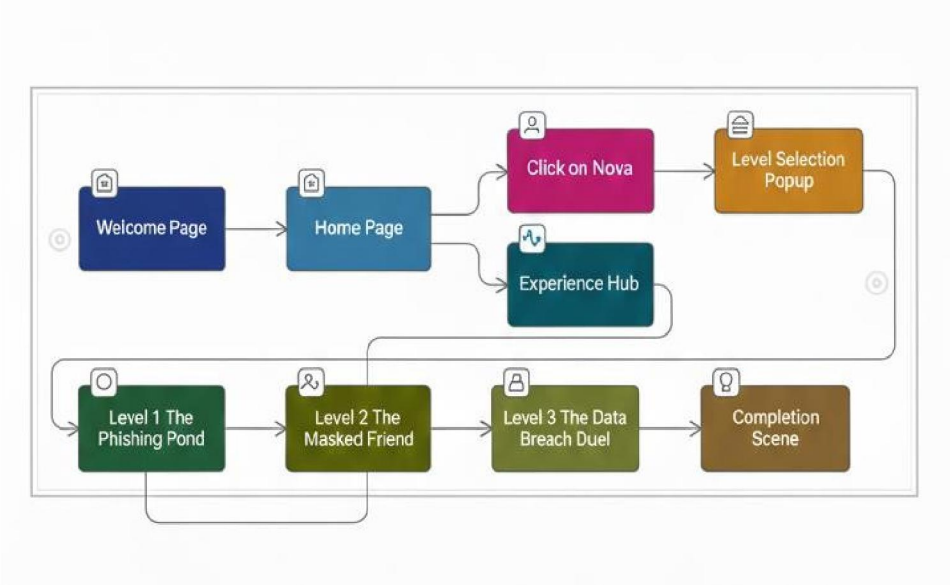


FIG.1 : Flow of the Game

2.3 Narrative and Level Design

The game is divided into three distinct phases:

League 1 The Phishing Pond(Telegraph Integrity): This introductory phase is centered on relating deceptive messaging. Players must separate between licit dispatches and vicious attempts from the antagonist Phishlor, manually filtering fraudulent data into a secure disposal zone.

League 2 The Trust Maze(Cerebral Adaptability): This stage shifts the focus to mortal-centric vulnerabilities. It requires actors to navigate a complex social simulation where they must descry and redirect sophisticated social engineering pushes and manipulative dialogue.

League 3 The Crystal Breach (Technical Fortification): The final challenge is a high haste specialized defense simulation. To guard the "Digital Crystal" from the adversary CipherShade, players must applymulti-factor authentication(MFA), emplace critical software updates, and enhance credential complexity under time- sensitive conditions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, December 2025
Impact Factor: 7.67

III. LITERATURE SURVEY

Current research in "Serious Games" shows that players retain up to 75% more information when they actively engage in problem-solving. Studies like SherLOCKED and PeriHack demonstrate that detective-themed stories increase the time users spend practicing security habits. CipherQuest builds on these findings by adding Adaptive Intelligence, which keeps the game relevant to the player's specific skill level.

• Active Participation: Integrated progression systems, such as tiered achievements and experience points, foster sustained user investment. These mechanics transform training into a high-engagement cognitive task, ensuring longer focus than static educational formats.

• Scenario-Based Learning: Games that simulate detective work or escape rooms help players learn problem-solving through discovery instead of memorization.

• Multimodal Learning: Blending narrative-driven scenarios with interactive visual puzzles accommodates diverse cognitive archetypes. This synergy optimizes mental processing and deepens knowledge retention by grounding abstract security rules in a cohesive story.

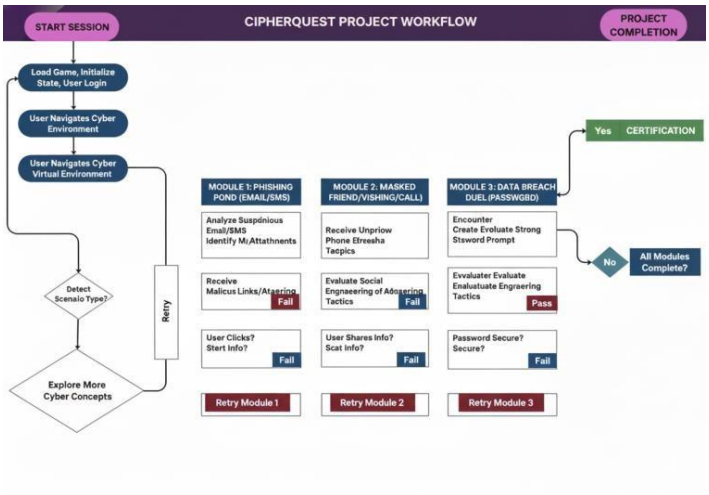
User Progression

To apply these principles, CipherQuest uses a structured flow. As outlined below, the application guides users from a central hub into specialized learning environments.

The progression starts at the Welcome Page and moves to a Home Page where users encounter branching options. They can choose to interact with Nova, the AI guide, or enter the Experience Hub. This leads to the Level Selection interface, which acts as the gateway to three main learning modules:

1. The Phishing Pond: Focused on email and link security.
2. The Masked Friend: Addressing social engineering and identity theft.
3. The Data Breach Duel: Simulating high-stakes incident response.

The journey ends with a Completion Scene that rewards users with badges and final scores, completing the gamification cycle described in the research.



IV. SYSTEM FEATURES

Beyond the main design, CipherQuest includes several engaging features aimed at keeping players involved over the long term. These features help players develop lasting digital habits:

- Adaptive Difficulty: The game's AI serves as a "Silent Proctor" that constantly assesses the user's skills. It tracks specific metrics, such as how long it takes for a player to spot a fraudulent URL or how accurately they respond under pressure. If a player shows expertise, the AI increases the challenge by adding more advanced

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, December 2025
Impact Factor: 7.67

decoys or shortening the response time. This helps maintain a state of "flow", where the difficulty level matches the player's improving skills, preventing boredom or excessive frustration.

- Reward System and Certification: To create a sense of progression and professional recognition, CipherQuest uses a tiered achievement system. As players move through the levels, they earn badges like "Phish-Free" or "Trust Wisely". After completing the final "Crystal Breach" level, players receive the distinguished "Cyber Guardian" rank. They also get a downloadable and shareable Cyber Safety Certificate, which acts as proof of their security knowledge, encouraging players to take pride in their ability to protect themselves online.
- Experience Hub: Recognizing that cybersecurity is a shared responsibility, the game features an Experience Hub. This community-focused platform is built into the game interface. Users can share real-life security experiences, such as convincing scams they encountered or breaches they observed, either anonymously or with their username. By learning from the experiences of others, players gain a wider understanding of the changing threat landscape, transforming the game from a solitary activity into a collaborative learning environment.

V. FUTURE SCOPE

While the current framework establishes a robust foundation, several technical trajectories exist to amplify its pedagogical reach and functional depth:

Collaborative SOC Defense: By evolving from a solo interface to a multi-agent framework, the system simulates the complexities of a Security Operation Center (SOC). The focus shifts from isolated troubleshooting to unified defensive protocols, requiring players to synchronize their responses against multi-vector incursions. This transition demonstrates that institutional security depends as much on interpersonal crisis coordination as it does on individual technical proficiency.

Predictive Behavioral Intelligence: By integrating sophisticated machine learning models, the platform could generate comprehensive "Vulnerability Heatmaps" for institutions. This deep-tier analytics suite would move beyond simple scoring to pinpoint specific conceptual gaps such as a workforce's susceptibility to social engineering versus technical misconfigurations. Such data-driven insights enable administrators to deploy surgical training interventions.

Immersive Spatial Defense (XR) :Integrating Extended Reality (XR) shifts cybersecurity training from a screen-based exercise to a spatially-aware experience. By navigating a high- fidelity 3D workspace, learners perform environmental risk assessments, identifying tangible threats such as "piggybacking" at secure entries or the presence of visible sensitive data. This kinesthetic approach embeds defensive routines into the user's physical intuition, ensuring that security responses become involuntary reactions rather than recalled facts.

Dynamic Threat Intelligence Synchronization: The system's relevance could be maintained through an API-driven link to global threat feeds. By ingesting real-time data on emerging malware and active phishing trends, the Threat Persona Engine (TPE) can dynamically generate puzzles based on actual incidents occurring in the wild. This "Live Training" model ensures the curriculum remains synchronized with the rapidly shifting global threat landscape.

VI. CONCLUSION

CipherQuest offers a scalable and engaging solution to the global cybersecurity skills shortage by completely rethinking how security education is delivered. It shifts the focus from passive listening, where users often forget information as soon as a video ends, to active defense. This approach empowers users to build muscle memory for digital safety. The platform puts users in a proactive role, teaching them to recognize and neutralize threats in a controlled environment. This prepares them before those same threats can cause irreversible damage to personal or organizational data.

The integration of the Threat Persona Engine (TPE) sets this project apart. It ensures that the learning process stays as dynamic and evolving as the cyber threats it aims to combat. Instead of facing static, predictable puzzles, players encounter adversaries that mimic the actual behaviors and strategies used by real-world hackers. This creates a "live" training experience that adapts to the player's skill level, ensuring that their knowledge is continuously tested and reinforced.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, December 2025 Impact Factor: 7.67

Ultimately, CipherQuest shows that gamification and adaptive intelligence can bridge the gap between awareness and action. It transforms the intimidating complexity of cybersecurity into a set of intuitive skills. This fosters a generation of "Cyber Guardians" who are not just informed but are also prepared to defend the digital frontier. By providing a safe space for trial and error, the system makes sure that when a user faces a sophisticated attack, it isn't their first time defending against it.

REFERENCES

[1]. affray, A., & Nurse, J. R. C. (2021). SherLOCKED: A Detective-Themed Serious Game for Cyber Security Education. arXiv:2107.04506.

[2]. Srivatanakul, T. (2024). Designing cybersecurity escape rooms: A gamified approach to learning. Journal of Cybersecurity Education, Research and Practice.

[3]. Jadhav, B. V. (2018). Enhancing Cybersecurity Skills by Creating Serious Games. Technical Research Journal, Computer Department.

[4]. Kumar, A., & Patel, J. (2019). Design and Evaluation of Cybersecurity Serious Games for Learning. International Journal of Serious Games.

[5]. Chen, L., & Roberts, M. (2018). Capture-the-Flag as an Educational Tool: Lessons from Practice. Proceedings of the Education for Conference.

[6]. Martinez, E., & Lee, J. (2020). Gamification and Learning Outcomes: A Review for Security Courses. Computers & Education.

[7]. Singh, R., & Gomez, P. (2017). Interactive Tutorials and Narrative in Security Education Games. IEEE Transactions on Learning Technologies.