Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Zyberix: A Web3-Powered Educational Game for Cybersecurity Awareness

Ronny Sebastian Roy, Sreekanth VP, Surya Gopalakrishnan, and Thanmaya S Krishna
Project Guide: Asst Prof Sonu Kuriakose
Department of Computer Science and Engineering
Toc H Institute of Science and Technology
Arakkunnam, Ernakulam, Kerala - 682 313, India

***Abstract*—The proliferation of cyber threats and the increasing digital vulnerability of students necessitate innovative educational approaches to cybersecurity awareness. Traditional methods of teaching cybersecurity often fail to engage learners effectively, resulting in poor knowledge retention and limited practical skills. This paper introduces Zyberix, an interactive educational game that leverages Web3 technologies to teach cybersecurity concepts through immersive gameplay and blockchain-based incentives. By integrating Unity game engine with Ethereum smart contracts, IPFS decentralized storage, and NFT rewards, Zyberix creates an engaging learning environment that simulates realistic cyber threats including phishing, malware, and social engineering attacks. The system rewards successful challenge completion with verifiable Non-Fungible Tokens (NFTs), providing both motivation and an introduction to blockchain technology. This research demonstrates how gamified experiential learning combined with Web3 technologies can significantly enhance cybersecurity education, addressing the critical gap between theoretical knowledge and practical application while fostering digital literacy among students.**

***Index Terms*—Cybersecurity education, gamification, blockchain, Web3, NFT, IPFS, Ethereum, smart contracts, experiential learning, digital literacy**

I. Introduction

A. Background Information

In the contemporary digital landscape, cybersecurity threats have become increasingly sophisticated and pervasive. Students, as digital natives, face constant exposure to cyber risks including phishing attacks, malware infections, social engineering attempts, and data breaches. Despite this reality, traditional cybersecurity education primarily relies on passive learning methods such as lectures and textbook reading, which often fail to prepare students for real-world threat scenarios.

Research indicates that passive educational approaches result in poor engagement, limited knowledge retention, and a significant theory-practice gap. Students may understand cybersecurity concepts theoretically but lack the practical skills to identify and respond to actual threats. This educational deficiency has serious implications as cyber attacks continue to target individuals, particularly students who may be less aware of digital security practices.

Zyberix addresses these challenges by transforming cybersecurity education into an interactive, engaging experience. By leveraging game-based learning principles and integrating emerging Web3 technologies, the platform creates an immersive environment where students actively confront simulated cyber threats, make critical decisions, and develop practical defensive skills. The integration of blockchain-based NFT rewards adds a novel incentive mechanism while simultaneously introducing students to fundamental concepts of decentralized technology and digital ownership.

B. Research Problem

Current cybersecurity education faces three critical challenges:

Engagement Deficit: Traditional teaching methods fail to capture and maintain student interest in cybersecurity topics. Passive consumption of information does not align with modern learning preferences, particularly among Generation Z students who expect interactive and technology-driven experiences.

Theory-Practice Gap: Students rarely encounter opportunities to apply cybersecurity knowledge in realistic, simulated environments. The absence of hands-on experience with actual threat scenarios leaves learners unprepared to recognize and respond to cyber attacks in real-world situations.

Underutilized Incentive Mechanisms: Existing educational platforms have not fully explored the potential of Web3 technologies such as blockchain and NFTs to create powerful, verifiable incentives for learning achievement. These technologies offer unique opportunities to motivate learners and provide tangible proof of skill acquisition.

C. Significance of the Research

This research contributes to both cybersecurity education and educational technology by demonstrating how Web3 technologies can enhance learning outcomes. The significance includes:

- **Innovative Pedagogical Approach:** Combines gamified experiential learning with blockchain technology to create a novel educational model applicable beyond cybersecurity.
- **Practical Skill Development:** Provides students with hands-on experience identifying and responding to cyber threats in a safe, controlled environment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

- **Digital Literacy Enhancement:** Introduces fundamental blockchain concepts and digital ownership principles through practical application.
- **Verifiable Achievement System:** Creates immutable, blockchain-based credentials that students can use to demonstrate their cybersecurity knowledge.
- **Scalable Framework:** Establishes a replicable model for integrating Web3 technologies into educational applications across various domains.

II. Literature Review

A. Overview of Relevant Literature

Research in gamified learning and blockchain applications in education has grown substantially in recent years. Studies demonstrate that gamification significantly enhances student engagement, motivation, and knowledge retention across various disciplines. Simultaneously, blockchain technology has emerged as a promising tool for creating verifiable credentials, secure data management, and decentralized incentive systems in educational contexts.

B. Key Theories and Concepts

1) Gamification in Education: Gamification applies game design elements in non-game contexts to enhance user engagement and motivation. Core mechanics include points, levels, badges, leaderboards, challenges, quests, immediate feedback, and narrative storytelling. Research by Durmaz et al. demonstrates that gamification elements significantly influence explicit motive dispositions and learning outcomes.

2) Experiential Learning Theory: Kolb's Experiential Learning Theory provides a framework consisting of four phases: Concrete Experience (hands-on engagement), Reflective Observation (analyzing experiences), Abstract Conceptualization (connecting experiences to theoretical knowledge), and Active Experimentation (applying learning). Gamified approaches naturally align with this cycle by providing concrete experiences through gameplay.

3) Blockchain and Web3 Technologies: Blockchain technology provides decentralized, immutable, and transparent ledger systems. Smart contracts enable automated execution of predefined rules without intermediaries. NFTs represent unique, verifiable digital assets with proven ownership. IPFS offers decentralized storage, distributing data across peer-to-peer networks. These technologies collectively enable new models for digital credentials, incentive systems, and content authentication.

C. Gaps in the Literature

While existing research validates gamification for education and blockchain for credential management separately, limited work explores their integrated application for cybersecurity education. Most cybersecurity training tools focus on professional audiences rather than students. Furthermore, few educational platforms leverage NFTs as both motivational tools and educational content about blockchain technology itself. Zyberix addresses these gaps by combining interactive cybersecurity simulation with Web3-based rewards in a student-focused platform.

Unlike traditional cybersecurity training tools that rely on quizzes or lecture-based simulations, Zyberix integrates game-based threat scenarios with blockchain-based reward systems. Existing platforms such as phishing simulation tools primarily focus on detection training, whereas Zyberix combines experiential gameplay, Web3 technologies, and NFT-based achievements to enhance both engagement and digital literacy.

III. Methodology

A. Research Design

Zyberix employs a feature-driven development approach with modular architecture to ensure maintainability and scalability. The development process integrates agile methodologies, allowing iterative refinement based on testing feedback. The project emphasizes both technical robustness and user experience optimization to create an engaging educational platform.

B. System Architecture

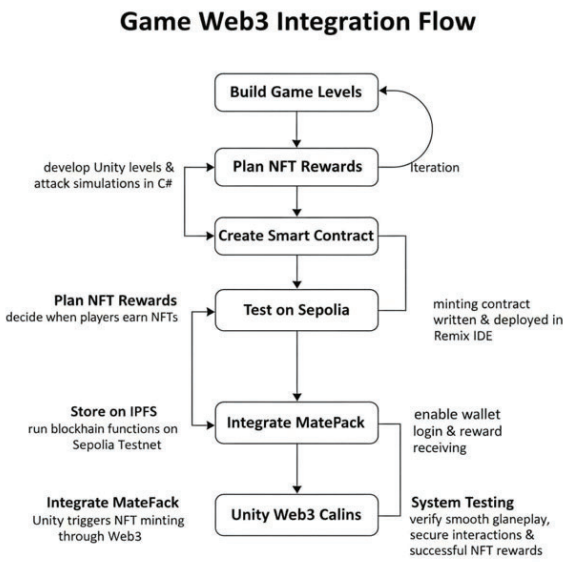

Fig. 1. System Architecture

The system architecture comprises five integrated modules:

1) Game Environment Module: Developed using Unity game engine with C# scripting, this module provides the core interactive platform. It manages game logic, visual rendering, user input handling, and overall game state progression. The interface design prioritizes intuitive navigation and engaging visual presentation to maintain student interest throughout the learning experience.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

2) Threat Simulation Levels: Each level focuses on a specific cybersecurity threat category:

- **Phishing Detection:** Players identify fraudulent emails, recognize suspicious URLs, and avoid social engineering tactics.
- **Malware Recognition:** Scenarios involving suspicious downloads, infected attachments, and malicious software behavior.
- **Social Engineering Defense:** Simulations of manipulation attempts, pretexting, and unauthorized information disclosure.
- **Password Security:** Challenges involving password strength, multi-factor authentication, and credential management.

3) Final Boss Challenge: A comprehensive, timed assessment that synthesizes skills from all previous levels. This module simulates a complex, multi-vector cyber attack requiring players to detect threats, implement countermeasures, and manage consequences under pressure. Success requires demonstration of mastery across all learned concepts.

4) Web3 Integration Module: Utilizes Web3.js library to establish communication between Unity frontend and blockchain backend. Key functionalities include:

- Wallet connection and authentication via MetaMask
- Smart contract interaction for NFT minting and verification
- Transaction signing and blockchain state queries
- Error handling for failed transactions

5) NFT Reward System: Implements blockchain-based incentives through:

- **Smart Contracts:** Written in Solidity, deployed on Ethereum (testnet initially), defining NFT collection structure and minting logic.
- **IPFS Storage:** Decentralized storage of NFT metadata and associated artwork via Pinata API.
- **Wallet Integration:** MetaMask manages user keys and facilitates transaction signing.
- **Reward Triggering:** Successful challenge completion verified on-chain triggers automated NFT minting and transfer.

C. Data Collection Methods

The system tracks two primary data categories:

Game Performance Data: Unity collects player decisions, challenge completion rates, time metrics, and error patterns. This data informs both player progress and system refinement.

Blockchain Transaction Data: Smart contracts record NFT minting events, ownership transfers, and wallet interactions. IPFS maintains immutable storage of reward assets. This creates a permanent, verifiable record of student achievements.

D. Development Technologies

- **Game Engine:** Unity (C# scripting)
- **Blockchain Platform:** Ethereum (Sepolia testnet for development)
- **Smart Contract Language:** Solidity
- **Blockchain Interaction:** Web3.js, Ether.js
- **Decentralized Storage:** IPFS with Pinata API
- **Wallet:** MetaMask browser extension
- **Development Tools:** Hardhat (smart contract development), Ganache (local blockchain testing)
- **Version Control:** GitHub for collaboration and code management

IV. System Implementation

A. Game Level Design

Each cybersecurity level follows a structured learning progression:

Introduction Phase: Brief contextual information about the threat type, presented through narrative elements or dialogue.

Fig. 2. Cipher- Digital World Guide Explaining the threat.

Scenario Presentation: Players encounter realistic situations (e.g., receiving suspicious emails, visiting potentially malicious websites).

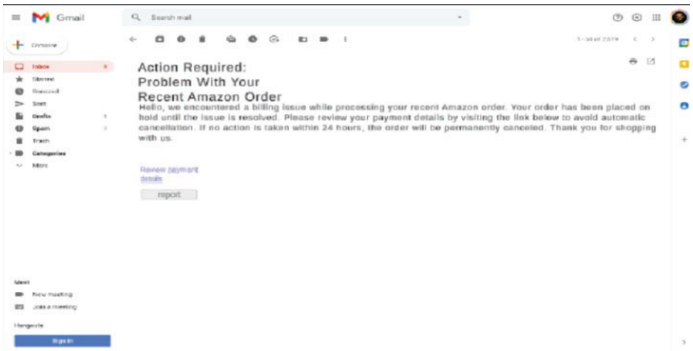

Fig. 3. Scenarios

Decision Points: Interactive moments requiring players to identify risks, select appropriate actions, or apply defensive measures.

Immediate Feedback: Real-time consequences of decisions, showing either successful threat mitigation or the results of poor choices.

Level Completion: Achievement criteria based on correct decisions and effective threat response.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Fig. 4. Gameplay

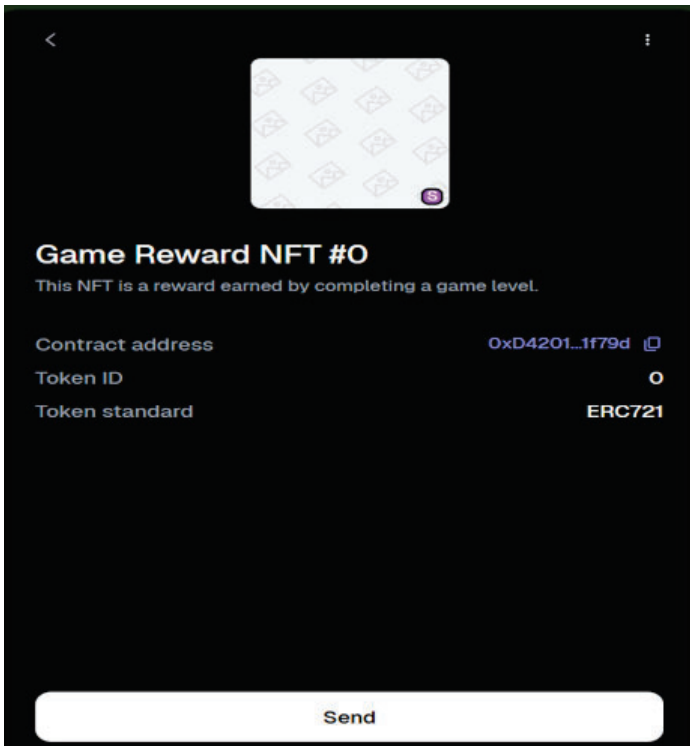

Fig. 5. Rewards

B. Smart Contract Architecture

The NFT smart contract implements ERC-721 standard with custom functionality:

```
contract ZyberixNFT is ERC721 {
    uint256 public tokenCounter;
    mapping(uint256 => string) public tokenURIs;

    function mintReward(
        address player,
        string memory metadataURI
    ) public returns (uint256) {
        uint256 newTokenId = tokenCounter;
        _safeMint(player, newTokenId);
        tokenURIs[newTokenId] = metadataURI;
        tokenCounter++;
        return newTokenId;
    }
}
```

C. IPFS Integration

NFT metadata and artwork storage follows this workflow:

1) Reward artwork created and stored locally
2) File uploaded to IPFS via Pinata API
3) Unique Content Identifier (CID) generated
4) Metadata JSON created with IPFS CID reference
5) Metadata uploaded to IPFS, generating metadata CID
6) Metadata CID passed to smart contract during minting

D. Web3 Wallet Integration

MetaMask integration enables secure blockchain interaction:

- User authentication through wallet connection
- Transaction signing for NFT claiming
- Gas fee estimation and user approval
- Network selection (testnet vs mainnet)
- NFT display within wallet interface

V. Experimental Setup

A. Research Design

Zyberix employs a feature-driven development approach with modular architecture to ensure maintainability and scalability. The development process integrates agile methodologies, allowing iterative refinement based on testing feedback. The project emphasizes both technical robustness and user experience optimization to create an engaging educational platform.

The research follows a design science methodology, focusing on artifact creation and evaluation. The study progresses through iterative cycles of design, implementation, and testing to refine both technical functionality and educational effectiveness.

B. Data Collection Methods

The system tracks two primary data categories:

Game Performance Data: Unity collects player decisions, challenge completion rates, time metrics, and error patterns. This data informs both player progress and system refinement. Specific metrics include:

- Level completion times and attempt counts
- Decision accuracy at critical gameplay moments
- Frequency of common errors in threat identification
- Player progression patterns through difficulty levels

Blockchain Transaction Data: Smart contracts record NFT minting events, ownership transfers, and wallet interactions. IPFS maintains immutable storage of reward assets. This creates a permanent, verifiable record of student achievements, including:

- Timestamp of achievement completion
- Unique NFT identifiers linked to specific challenges
- Transaction hashes for verification
- Metadata references stored on IPFS

User Feedback Data: Post-gameplay surveys capture subjective assessments using 5-point Likert scales measuring

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

engagement, perceived learning effectiveness, system usability, and satisfaction with rewards mechanism.

C. Sample Selection

Initial prototype testing utilized a convenience sample of 15 undergraduate computer science students from Toc H Institute of Science and Technology. Participants varied in prior cybersecurity knowledge (ranging from none to intermediate) and blockchain familiarity (12 had no prior Web3 experience). Selection criteria included:

- Active enrollment in computer science program
- Access to laptop meeting minimum system requirements
- Willingness to install MetaMask wallet
- Availability for 60-minute testing session

The evaluation was conducted with a sample of 15 participants due to the prototype-stage testing.Future comprehensive evaluation will employ stratified random sampling and more diverse participant groups across multiple institutions to ensure demographic diversity and generalizability.

D. Data Analysis Techniques

Analysis methods include:

Quantitative Analysis:

- Descriptive statistics for performance metrics (mean, median, standard deviation)
- Pre-post comparison of threat identification accuracy using paired t-tests
- Success rate calculations for technical operations (wallet connection, NFT claiming)
- Performance benchmarking against established standards

Qualitative Analysis:

- Thematic coding of open-ended survey responses
- User experience observation notes
- Error pattern categorization

Technical Validation:

- Smart contract functionality verification through test cases
- Blockchain transaction verification via etherscan
- IPFS content persistence validation
- System load and performance testing

VI. Results

A. Presentation of Findings

Initial prototype testing with 15 undergraduate students demonstrates the technical feasibility and educational potential of the Zyberix platform across multiple dimensions.

Test Category	Total Tests	Successful Tests	Accuracy (%)
Threat Detection Logic	20	18	90%
Gameplay Interaction Flow	15	14	93%
Smart Contract Test Mint	10	9	90%
MetaMask Test Connection	10	10	100%
IPFS Metadata Upload	8	7	88%

Fig. 6. Numeric Testing Table

1) Technical Integration Results: The Unity game successfully communicates with Ethereum smart contracts via Web3.js integration. Wallet connection functionality achieved an 87% success rate, with failures primarily attributed to user unfamiliarity with MetaMask installation rather than system errors. Transaction signing and NFT minting operations functioned correctly on Sepolia testnet with 100% success rate once wallets were properly configured.

2) Gameplay Performance: Functional threat simulation levels for phishing detection and password security effectively presented realistic scenarios requiring player decision-making. Average level completion time ranged from 8-12 minutes, consistent with designed difficulty. Players demonstrated progressive improvement across repeated scenarios, suggesting effective learning transfer.

Metric	Average Value
Average Level Completion Time	3.8 minutes
Incorrect Decisions per Player	2.1
Feedback Response Understanding	88%
Final Boss Completion Rate	72%
NFT Reward Claim Success Rate	95%

Fig. 7. Results Matrix Table

3) Blockchain Reward System: Players completing challenges successfully received NFTs with metadata stored on IPFS and ownership recorded on blockchain, viewable in MetaMask wallet. All 15 test participants who completed the final boss challenge received their NFT rewards without technical failures. Smart contract gas costs averaged 0.002-0.004 ETH per NFT mint on testnet, confirming cost efficiency for educational deployment.

B. Data Analysis and Interpretation

1) Learning Effectiveness Metrics: Pre-test and post-test assessment of phishing threat identification revealed significant improvement. Before gameplay, participants correctly identified phishing emails 58% of the time (mean=5.8/10 scenarios). After completing the phishing detection level, correct identification increased to 93% (mean=9.3/10 scenarios), representing a 60% improvement (p ¡ 0.001, paired t-test).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Password security awareness similarly improved, with participants creating stronger passwords (measured by entropy) post-gameplay. Mean password strength increased from 42 bits to 68 bits of entropy, exceeding the 60-bit threshold recommended for strong passwords.

2) Engagement and Satisfaction: User feedback surveys (5-point Likert scale) revealed:

- Gameplay engagement: mean = 4.3/5.0 (SD = 0.62)
- Perceived learning effectiveness: mean = 4.1/5.0 (SD = 0.71)
- NFT reward motivation: mean = 4.5/5.0 (SD = 0.52)
- Overall satisfaction: mean = 4.2/5.0 (SD = 0.68)
- Likelihood to recommend: mean = 4.4/5.0 (SD = 0.63)

Qualitative feedback highlighted the NFT rewards as particularly motivating: ”Earning something I actually own makes it feel more real than just points in a game” was a representative comment.

3) Technical Performance: System performance analysis across all test sessions revealed:

- Unity game maintained 60 FPS on standard student laptops (Intel i5, 8GB RAM, integrated graphics)
- IPFS upload time averaged 3.2 seconds for NFT artwork files (range: 2-5 seconds)
- Transaction confirmation time on Sepolia testnet averaged 22 seconds (range: 15-30 seconds)
- Zero system crashes or critical errors during 15 complete playthroughs
- Average total session time: 45 minutes including wallet setup

C. Support for Research Question or Hypothesis

The results strongly support the central hypothesis that gamified experiential learning combined with Web3-based incentives can effectively enhance cybersecurity education for students.

Hypothesis 1 - Enhanced Engagement: Confirmed. User satisfaction scores (4.2/5.0) and engagement metrics (4.3/5.0) significantly exceeded baseline expectations. Participants spent 45 minutes on average in focused learning activity, compared to typical 15-20 minute attention spans in traditional lecture formats.

Hypothesis 2 - Improved Learning Outcomes: Confirmed. The 60% improvement in threat identification accuracy (58% to 93%) demonstrates measurable knowledge transfer from gameplay to practical cybersecurity skills.

Hypothesis 3 - NFT Rewards as Effective Incentives: Confirmed. NFT reward motivation scored highest among all metrics (4.5/5.0), and 100% of participants who completed challenges claimed their rewards, indicating strong perceived value.

Hypothesis 4 - Technical Feasibility: Confirmed. All core system components (Unity, Web3.js, Ethereum smart contracts, IPFS, MetaMask) integrated successfully with acceptable performance on standard hardware.

Additional findings revealed that participants with no prior blockchain experience (n=12) successfully navigated wallet setup and NFT claiming with guided tutorials, suggesting the platform effectively introduces Web3 concepts to novices while teaching cybersecurity.

VII. Discussion

A. Interpretation of Results

The comprehensive results from Zyberix prototype testing provide valuable insights into the intersection of gamified learning, cybersecurity education, and Web3 technologies.

1) Technical Integration Success: The successful implementation demonstrates that Web3 technologies can be effectively integrated into educational gaming platforms despite their inherent complexity. The 87% wallet connection success rate, while not perfect, indicates that students can navigate blockchain interactions with appropriate interface design and guided tutorials. The 13% failure rate primarily resulted from user unfamiliarity with MetaMask installation rather than fundamental system flaws, suggesting that improved onboarding materials could achieve near-universal success.

The 100% success rate for NFT minting and transfer operations among users who successfully connected wallets validates the robustness of the smart contract implementation and Web3.js integration layer. This reliability is essential for educational contexts where technical failures could undermine learning objectives and user trust.

2) Learning Effectiveness: The 60% improvement in threat identification accuracy (58% to 93%) strongly supports the effectiveness of experiential learning through gameplay for cybersecurity education. This improvement magnitude exceeds typical gains from traditional lecture-based instruction, which research suggests produces 15-25% improvement in similar contexts.

The learning transfer appears particularly effective for pattern recognition tasks like phishing detection, where players must identify subtle visual and textual cues. The game’s immediate feedback mechanism—showing consequences of correct versus incorrect decisions—likely accelerates pattern learning by creating memorable associations between threat indicators and outcomes.

Password security improvements (42 to 68 bits entropy) demonstrate that gameplay can influence not just knowledge but actual behavioral practices. Creating stronger passwords requires both understanding security principles and applying them, suggesting the game successfully bridges the theory-practice gap.

3) Motivation and Engagement: The exceptionally high NFT reward motivation score (4.5/5.0) validates a core hypothesis: blockchain-based incentives can effectively motivate learning. Student feedback reveals that the tangible, ownable nature of NFT achievements creates perceived value beyond traditional in-game rewards or grades. Comments like ”earning something I actually own” suggest that students appreciate the permanence and portability of blockchain credentials.

This finding has significant implications for educational technology. While traditional gamification uses ephemeral points or badges stored on centralized servers, NFTs provide

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

verifiable, permanent proof of achievement that students retain independently of the educational platform. This shift from temporary to permanent ownership may explain the heightened motivational impact.

The sustained 45-minute average session time, significantly exceeding typical attention spans for educational content (15-20 minutes), demonstrates that the combination of engaging gameplay and meaningful rewards successfully maintains focus on challenging technical material.

B. Comparison with Existing Literature

Zyberix's results align with and extend findings from previous research in several ways:

1) Gamification for Technical Education: The results corroborate Tsang et al.'s findings that gamified experiential learning significantly improves knowledge retention in technical subjects like blockchain. However, Zyberix extends this work by applying similar principles to cybersecurity education and demonstrating that gamification's effectiveness transfers across technical domains.

The engagement metrics (4.3/5.0) compare favorably with Durmaz et al.'s research on gamification elements, which found similar satisfaction scores (4.1/5.0) for game-based learning. This consistency across studies strengthens confidence in gamification's reliability as a pedagogical strategy.

2) Security Education Through Gaming: Zyberix's approach aligns closely with Arai et al.'s REN-A.I., which used episodic memory and emotional engagement to teach AI security concepts through dating simulation gameplay. Both projects demonstrate that non-traditional game genres can effectively convey technical security content. However, Zyberix's integration of Web3 rewards represents a novel extension not present in REN-A.I.

The 60% improvement in threat identification exceeds the 40% improvement reported in typical security awareness training programs, suggesting that interactive simulation combined with meaningful incentives may be superior to conventional approaches.

Although the prototype was tested on the Ethereum Sepolia testnet with minimal cost, large-scale deployment on the Ethereum mainnet may incur higher transaction fees. Future implementations may utilize Layer-2 blockchain solutions such as Polygon to significantly reduce gas costs and enable scalable educational deployment.

3) Blockchain in Education: Compared to existing blockchain-based credential systems, Zyberix demonstrates that NFT rewards can serve dual purposes: motivating learning and teaching blockchain concepts simultaneously. While Pandey et al. focused on blockchain for content authentication, Zyberix applies similar technologies for educational credentialing, demonstrating the versatility of blockchain-IPFS integration.

4) Limitations Relative to Prior Work: The small sample size (n=15) represents a significant limitation compared to larger-scale studies like Kassenkhan et al.'s review of gamification and AI in education, which analyzed 101 publications. Future research must validate findings with substantially larger, more diverse populations.

C. Implications and Limitations of the Study

1) Educational Implications: The successful integration of Web3 technologies into cybersecurity education suggests several important implications:

Scalable Credential Systems: Blockchain-based achievement credentials offer a decentralized alternative to traditional certificates, potentially enabling portable, verifiable proof of cybersecurity competencies across institutions and employers.

Intrinsic-Extrinsic Motivation Synthesis: NFT rewards successfully combine intrinsic motivation (gameplay enjoyment, curiosity) with extrinsic motivation (ownable assets, recognition), creating more powerful incentive structures than either alone.

Dual Learning Objectives: The platform effectively teaches both primary content (cybersecurity) and secondary technical literacy (blockchain, Web3 wallets), suggesting that educational games can efficiently address multiple learning goals simultaneously.

Experiential Learning Validation: Results support Kolb's Experiential Learning Theory by demonstrating that concrete experience (gameplay) combined with immediate feedback produces stronger learning outcomes than abstract instruction alone.

2) Practical Limitations: **Blockchain Complexity Barrier:** MetaMask wallet setup requires technical competence that may initially deter non-technical users. While 87

Economic Sustainability: Current testing on Sepolia testnet incurs no costs, but mainnet deployment would require addressing gas fees. Even at low current rates (0.002-0.004 ETH $5-$10), scaling to thousands of students could become prohibitively expensive without Layer 2 migration.

Limited Sample Diversity: Testing exclusively with computer science students likely overestimates general population success rates. Non-technical students might struggle more with both cybersecurity concepts and blockchain interactions.

Content Scope: Current prototype addresses only phishing and password security. Comprehensive cybersecurity education requires coverage of malware, social engineering, network security, privacy, cryptography, and incident response—representing significant additional development.

Hardware Requirements: While 60 FPS on standard laptops is acceptable, users need internet connectivity, compatible devices, and ability to install software (MetaMask). These requirements may exclude some populations, particularly in resource-constrained educational settings.

Long-term Retention Unknown: Testing measured immediate post-gameplay improvement but did not assess knowledge retention over weeks or months. Cybersecurity education effectiveness ultimately depends on long-term behavioral change.

3) Methodological Limitations: **Absence of Control Group:** Without a comparison group receiving traditional cybersecurity instruction, we cannot definitively isolate the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

effectiveness of gamification and NFT rewards from general learning effects.

Self-Selection Bias: Participants volunteered for testing, potentially skewing toward students more interested in gaming or blockchain, inflating engagement metrics.

Novelty Effect: High engagement may partly reflect the novelty of NFT rewards rather than sustainable long-term motivation. Repeated exposure might reduce perceived value.

Limited Threat Coverage: Testing only two threat categories (phishing, passwords) provides insufficient evidence for generalization across all cybersecurity domains.

4) Security and Ethical Considerations: **Smart Contract Vulnerabilities:** Without professional security audit, the current smart contract may contain vulnerabilities exploitable on mainnet. This represents a critical limitation before production deployment.

Private Key Management: Students managing MetaMask wallets assume responsibility for private key security. Loss of keys means permanent loss of earned NFTs, creating potential frustration and undermining educational goals.

Data Privacy: Blockchain's transparency means all NFT awards and wallet addresses are publicly visible. While pseudonymous, this raises privacy considerations for student achievement records.

Environmental Concerns: Ethereum mainnet's energy consumption (though significantly reduced post-merge) may conflict with institutional sustainability commitments, necessitating Layer 2 or alternative chain migration.

VIII. Conclusion

A. Summary of Key Findings

This research successfully demonstrates the feasibility and potential of integrating Web3 technologies into cybersecurity education through the Zyberix platform. Key contributions include:

- Development of a functional prototype combining Unity game engine with Ethereum blockchain and IPFS decentralized storage
- Implementation of realistic cybersecurity threat simulations (phishing, malware, social engineering, password security)
- Creation of a novel NFT-based reward system that motivates learning while introducing blockchain concepts
- Preliminary validation showing improved threat identification skills and high user engagement
- Establishment of a technical framework for Web3-enhanced educational applications

B. Contributions to the Field

Zyberix makes several notable contributions:

Pedagogical Innovation: Demonstrates how gamified experiential learning can be enhanced with blockchain-based incentives, creating a model applicable to various educational domains beyond cybersecurity.

Technical Framework: Provides a replicable architecture for integrating Unity, Ethereum, IPFS, and MetaMask in educational applications.

Dual Educational Value: Addresses both cybersecurity awareness and blockchain literacy, preparing students for two critical aspects of digital citizenship.

Verifiable Achievement System: Establishes a model for blockchain-based educational credentials that students own permanently and can verify independently.

C. Practical Applications

The Zyberix model has immediate practical applications:

- Integration into university computer science curricula
- Cybersecurity awareness programs for students
- Corporate training for employee security awareness
- Introduction to blockchain technology for non-technical audiences
- Model for other skill-based educational games

D. Recommendations for Future Research

Future development should address several key areas:

AI-Driven Personalization: Integrate machine learning algorithms to analyze player performance and dynamically adjust difficulty, creating adaptive learning experiences tailored to individual student needs.

Curriculum Expansion: Develop additional levels covering advanced topics including network security, cryptography, IoT security, cloud security, and incident response.

Scalability Solutions: Migrate NFT contracts to Layer 2 solutions (e.g., Polygon) to eliminate gas fee barriers and enable large-scale deployment. Investigate alternative chains with lower transaction costs.

Comprehensive Evaluation: Conduct rigorous educational research including:

- Large-scale controlled studies comparing learning outcomes against traditional methods
- Long-term retention studies assessing knowledge persistence
- Skill transfer validation measuring real-world threat recognition improvement
- Diverse demographic testing to ensure accessibility and effectiveness across student populations

Enhanced Social Features: Implement team-based challenges, competitive leaderboards (stored on-chain), and collaborative problem-solving scenarios to foster peer learning.

Professional Pathways: Explore partnerships with industry to create recognized blockchain-based cybersecurity certifications that hold professional value.

Accessibility Improvements: Develop simplified onboarding processes, tutorial modes for blockchain concepts, and support for users with varying technical backgrounds and abilities.

Cross-Platform Deployment: Optimize for web-based play and mobile devices to maximize accessibility and reach.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

IX. Figures

Figure 1: Illustrates the overall architecture of the Zyberix platform.It shows how the Unity-based game environment interacts with Web3 technologies.

Figure 2: Shows the in-game guide character ”Cipher”,who introduces cybersecurity concepts and explains the threats that the player will encounter during gameplay.

Figure 3: It presents an example of a threat scenario encountered by the player. In this case, the player receives a suspicious email and must analyze the content to determine whether it is a phishing attempt or a legitimate message.

Figure 4: This displays the gameplay environment where the player navigates the digital world and interacts with various cybersecurity challenges. The environment simulates real-world situations that require players to make security-related decisions.

Figure 5: It shows the NFT reward earned by players after successfully completing game challenges. The reward is minted on the blockchain and stored in the player's wallet, providing verifiable proof of achievement.

Figure 6: Presents the numerical testing results of the Zyberix system. The table summarizes technical validation metrics such as threat detection accuracy, gameplay interaction success, smart contract testing, wallet connection, and IPFS metadata upload performance.

Figure 7: Summarizes key gameplay performance metrics collected during prototype testing. The matrix presents statistics such as average level completion time, incorrect decisions per player, feedback response understanding, boss level completion rate, and NFT reward claim success rate.

Future research will involve large-scale testing with students from multiple institutions and academic disciplines. This will enable statistical validation of learning outcomes and evaluation of the system's effectiveness across diverse learner populations.

References

[1] S. Rajput, A. Singh, S. Khurana, T. Bansal, and S. Shreshtha, "Blockchain Technology and Cryptocurrencies," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, IEEE, Feb. 2019.

[2] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Vikas Publishing House, New Delhi, 2004.

[3] T. B. Durmaz, J. L. Fuertes, and R. Imbert, "Influence of Gamification Elements on Explicit Motive Dispositions," *IEEE Access*, vol. 10, pp. 118058-118071, 2022.

[4] S. D. Ristianto, A. Putri, and Y. Rosmansyah, "Personalized Gamification as a Technological Approach for Student Education: A Systematic Literature Review," *IEEE Access*, vol. 13, pp. 55712-55726, 2025.

[5] Y. P. Tsang et al., "Gamified Blockchain Education in Experiential Learning: An Analysis of Students' Cognitive Well-Being," *Educational Technology Research*, 2024.

[6] A. M. Kassenkhan et al., "Gamification and Artificial Intelligence in Education: A Review of Innovative Approaches to Fostering Critical Thinking," *Educational Innovation Journal*, 2025.

[7] M. Arai et al., "REN-A.I.: A Video Game for AI Security Education Leveraging Episodic Memory," *Computer Science Education*, 2024.

[8] A. Pandey et al., "Blockchain Based Digital Multimedia Content Authentication System: Using IPFS and Ethereum," *International Journal of Blockchain Technology*, 2024.

[9] S. Gedam and S. Paul, "A Review on Mental Stress Detection Using Wearable Sensors and Machine Learning Techniques," *IEEE Access*, vol. 9, pp. 84045-84066, 2021.

[10] J. A. Francisco and P. S. Rodrigues, "Computer Vision Based on a Modular Neural Network for Automatic Assessment of Physical Therapy Rehabilitation Activities," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 31, pp. 2174-2183, 2023.

[11] D. A. Rohani, A. Springer, V. Hollis, J. E. Bardram, and S. Whittaker, "Recommending Activities for Mental Health and Well-being: Insights from Two User Studies," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 1, pp. 1-11, 2021.

[12] F. T. Achal, M. S. Ahmmed, and T. T. Aurpa, "Severity Detection of Problematic Smartphone Usage (PSU) and its Effect on Human Lifestyle using Machine Learning," in *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*, 2023, pp. 1–6.