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

CyberScape: A Gamified Simulation-Based Approach for Practical Cybersecurity Awareness and Education

Divya Ajay Ambre, Ayush Ashutosh Marale, Astha Vaibhav Narkhede
Mrs. Sonal Jogdand, Rajkumar Dilip Salunke
Department of Computer Engineering
Pimpri Chinchwad Polytecnic, Pune, India
divyaambre21@gmail.com, asthanarkhede@gmail.com, sonal.jogdand@gmail.com
salunkeraj68@gmail.com, ayush.marale@gmail.com

Abstract: *Due to the rapid development of digital technology, cyber-security threats like phishing, smishing, vishing, malware attacks, poor password practices, and social engineering attacks have become pervasive, especially among nontechnical individuals. Traditional cyber-security training, encompassing lectures, tutorial sessions, and awareness camps, typically fail to provide the requisite real-world experience required to effectively counter cyber-security threats. This presents a problem, causing ineffectual participation and lack of retention of key cyber-security concepts.This report presents CyberScape, an interactive cyber-security training platform developed using Unity, a popular computer game development platform, conceived to address these problems. CyberScape uses the Serious Gaming approach, simulating real-life cyber-attack scenarios in a virtual environment. Students embark on a complex virtual journey, with each level on the virtual journey focusing on a different cyber-security topic, such as identifying phishing attacks, protecting passwords, defending against USB malware attacks, Smishing, Vishing, and physical cybersecurity. Scenario-based, quiz, and decision-making tasks allow for effective experiential learning and encourage the adoption of appropriate cyber-security practices based on instant feedback.*

Keywords: Cybersecurity awareness, Gamification, Serious games, Experiential learning, Phishing and social engineering, Interactive simulation.

I. INTRODUCTION

As online services are increasing at a rapid pace, online threats too are becoming more common, thereby affecting people, organizations, and critical infrastructure around the globe. These threats, ranging from phishing, smishing, vishing, malware attacks, exploitation of weak passwords, as well as social engineering, still target human vulnerabilities rather than technological vulnerabilities. Even with increased efforts in enhancing security systems, human errors are still a main reason for a successful online attack, resulting in sensitive information leakage, monetary loss, and compromised personal information. Research indicates that most online attacks arise from users failure to identify and respond appropriately to online deceptive messages [1].

Contemporary methods of cybersecurity education, including classroom teaching, static tutorials, and education campaigns, usually consist of theoretical knowledge and do not provide an adequate opportunity for hands-on learning. Since cybersecurity education does not provide adequate opportunities for hands-on learning and usually an insufficient simulation of actual attack scenarios, it leaves learners with insufficient opportunities to apply theoretical concepts into actual defensive measures against cyberattacks [2].

To overcome the shortcomings, the use of experiential learning and gamification has emerged as an efficient tool for cybersecurity education. Simulated games based on serious contexts offer the advantage of engaging the participants in realistic scenarios, contributing to the development of practical skills like problem-solving, decision-making, and

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

learning through behavioral aspects. By familiarizing the users with a simulated attack experience similar to the real environment, the process efficiently increases the awareness levels and retention rates for the knowledge related to cybersecurity [3].

In this regard, the concept of CyberScape has been established in the context of this research, which is an interactive and game-based cybersecurity education platform developed using the Unity game engine. This platform, CyberScape, simulates a cyber world with real-life cyber threat simulations, wherein each level of the simulation focuses on various cybersecurity concerns, including phishing, protecting passwords, protecting from USB malware, smishing, vishing, and physical securities.

1.1 Background

The rising trends in the digital age have led to increasing cyber threats by exploiting vulnerabilities in humans through phishing/smishing/vishing attacks, malware attacks, as well as social engineering attacks by masquerading as someone trustworthy or a known firm. These have been resulting in serious losses in terms of money and sensitive information [1][2]. The rising trends in cyber attacks with more realistic and intelligent approaches like typical email attacks or social communication attacks make the previous methods of awareness inadequate for dealing with ever-changing cyber threats [3].

Although the traditional method of cybersecurity awareness education and use of static educational material is well in practice and adopted on a large scale, they often fail to deliver a direct experience concerning real-world attack situations. Learning through an inactive process holds back the ability to recognize and respond to a real attack and act appropriately in the real environment. As a consequence, the individual is still vulnerable to new and unexpected cyber threats despite gaining theoretical knowledge [4][6].

The proposed research is nested in the development of immersive and scenario-based awareness systems for cybersecurity. The proposed approach uses gamified simulations to expose learners to different types of cyber risks and attack scenarios including phishing, use of passwords, USB malware, and social engineering. The proposed system aims to improve awareness and dynamic actions on cybersecurity knowledge and risks through participation and decision-making efforts [5].

1.2 Contribution of this work

This report presents an overall plan for effectively improving cyber security knowledge by using active learning procedures with the help of games. Unlike other typical methods for learning cyber security that rely on lecturing, tutorials, or simple quizzes, the proposed approach seeks to address the drawbacks of passive learning methods by designing interactive games with real-life challenges. In most cases, other methods may lack the reality, flexibility, or interaction associated with real life, rendering them ineffective in preparing an individual for dealing with real cyber security issues.

Current training solutions may have provided the necessary theoretical knowledge, but they may not have the capability to simulate real-world scenarios such as phishing, smishing, phone, password, USB drop attacks, and physical security breaches. It is also likely that the systems were not incorporating consequence features to promote the precise selection with effective memory and modification.This effort represents an advancement in the area of cybersecurity education with the introduction of the CyberScape serious gaming platform, with its various innovations.

- Scenario-based cybersecurity awareness trainings: Including real life cybersecurity scenarios like Phishing, Smishing, Vishing, Password security, USB MALWARE Attacks, and Physical Security, which help train the users by actually involving them in the decision-making process.
- Interactive Learning Environment: Incorporating the use of gaming elements such as level advancement, quests, immediate feedback, or badges in order to increase student engagement.
- Developing an immersive simulation environment using Unity: Developing a first-person simulation environment that mimics real-world contexts and lets users explore simulated cybersecurity scenarios in a secure and virtual way.

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

- A Multi-Modal Learning Approach: Integrating pictorials, textual problems, audio situations, and assessment tasks that appeal to diverse learning styles and help improve memory recall.
- Training on awareness with a behavior-oriented approach: The training should focus on improving the user's behavior and decision-making capabilities instead of merely conveying knowledge to increase awareness on the applications of cybersecurity practices.

II. PROPOSED METHODOLOGY

This study proposes a new awareness system called CyberScape, designed as an immersive and gamified tool for improving the efficiency and effectiveness of the current approaches used in educating people on matters pertaining to the field of cyber security. The proposed system will provide a hands-on approach combined with instant feedback for improving the comprehension and decision-making skills of the user under real-life cyber threat conditions. This will be explained further below.

1. System Architecture

The proposed framework for CyberScape has the following essential components:

Interactive Simulation Environment:

The virtual reality environment developed using Unity, where participants can traverse a multi-level structure with first-person perspective. At each level, there are specified cybersecurity regions such as the awareness of phishing, securing passwords, smishing, vishing, USB malware attacks, and physical security. The activities are registered using proximity triggers and interactions.

Scenario-Based Cybersecurity Modules:

In addition, each of the principles of cybersecurity has an isolated scenario module. Examples include phishing identification messages, SMS fraudulent activity identification, voice-enabled telephone scam simulations, password strength evaluation, USB drop attack simulations, and physical document processing procedures. Specific scenarios are designed to test like actual scenarios in terms of cyber threats, requiring the user to make decisions[5][6].

Decision Evaluation and Logic Engine:

In real-time, the choices made by the user are judged through rules and standards that are pre-set. The actions are immediately identified as correct or incorrect, hence helping the user in understanding the outcomes of the choices he has made. This module determines the scenarios and progress.

Feedback and Learning Reinforcement Mechanism:

Immediate feedback is preferably given through visual, auditory, and written forms. Such reinforcement encourages good practices in cyberspace and emphasizes common signs of possible attacks, thereby allowing trainees to eliminate misunderstandings.

Progress Tracking and User Performance Assessment:

User engagement, the completion status of scenarios, and decision-making outcomes have also been recorded to assess the effectiveness of learning. This data provides insight into the structured approach adopted in the game and can also be used to assess improvements in cybersecurity awareness.

The new model combines immersion simulation, scenario tasks, and feedback to provide an efficient, interactive, and dynamic cybersecurity training experience. The new model relates theory to practical implementation, improving cyber security practices and promoting responsible actions among users.

2. Workflow

The document describes the overall process involving the proposed CyberScape system, which is end-to-end based.

- User Interaction: This is where the user navigates a virtual world made through Unity. The user interacts with various features available like objects, terminals, phones, emails, messages, and even real-world objects such as USB drives and physical documents. Each time, the user faces a cybersecurity scenario relevant to the learning module.

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

- Scenario Activation and Analysis: A specific cybersecurity scenario, such as phishing identification, smishing detection, password analysis, or USB attack simulation, will be triggered depending on user interactions. The system will analyze the inputs provided by the user.
- Decision Evaluation and Feedback: The actions made by the user would be measured against the right cyber-security practices. Immediate feedback regarding whether the action was safe or potentially dangerous would be provided through visual indications, auditory cues, and in writing.
- Learning Reinforcement and Progression: Correct choices help the player move to the next task or level, while wrong actions give a corrective response. This cyclical process of correction reinforces learning and refines problem-solving skills over time.

III. LEARNING CONTENT AND SCENARIO DESIGN

It makes use of several educational materials and virtual environments that ensure comprehensive knowledge about cybersecurity:

- Phishing and Smishing Scenarios: Email and SMS scams are simulated based on real-world phishing to help users recognize deceptive cues.
- Password Security Challenges: Interactive password security and breach scenarios that help in teaching the creation of secure passwords and credential awareness.
- Vishing and Phone Scam Simulations: In audio-based phone call scenarios, individuals would have to make decisions to receive or reject calls from supposedly genuine organizations.
- USB and Physical Security Scenarios: Playing out simulations such as handling unidentified USB devices, destruction of documents, and improper handling of notes to improve sound physical cybersecurity easures.

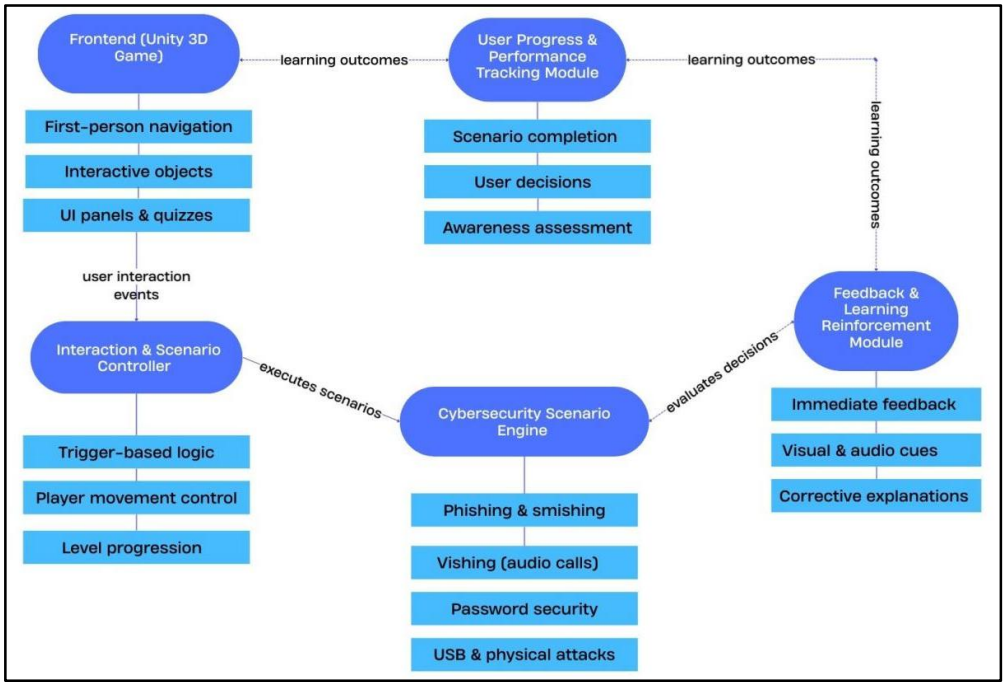

Fig.2: Architectural Diagram

IV. LITERATURE SURVEY

Recently, cybersecurity education and awareness have attracted immense attention due to the increased frequency and sophistication of cyber threats. Various methods for improving users' understanding, engagement, and response 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

online threats have been explored through research. Significant methodologies and contributions regarding this study are briefly overviewed below.

Traditional Awareness and Training Methods

Traditional cybersecurity education relies on lectures, demonstrations, static guidelines, and rapid assessments. Although these approaches are helpful in teaching theoretical concepts, they often lack enabling learners to acquire hands-on experience through realistic cyber-attack scenarios. Hence, although learners may theoretically comprehend cybersecurity concepts, they may struggle to apply them in real-life settings. On the other hand, passive learning approaches yield low engagement and weak retentiveness of cybersecurity practices, as research has shown [4][5].

Gamification in Cybersecurity Education

Gamification has now become a potent tool to enhance learner participation and engagement in cybersecurity education. Points, levels, challenges, and rewards integrated into the gamified systems promote active participation and sustained interest. Several studies show that game-based learning environments significantly improve knowledge retention and user interaction compared to traditional teaching methods. The acquisition of knowledge by means of learning through escape rooms and puzzles, particularly in cybersecurity studies, has proved successful in teaching concepts based on problem solving and learning by discovery [6].

Serious Games and Scenario-Based Learning

Interactive simulations reproduce real-life scenarios in secure environments, letting the learner acquire information by trying and making mistakes without suffering from any real-life consequences. It has been seen that detective-themed games, virtual escape rooms, and cybersecurity simulations have been used both in educational and enterprise environments, enhancing the learning and decision-making capabilities of participants [7]. These types of systems are based on learning by experience, not on pure memorization.

Multimedia and Multi-Modal Learning Approaches

Combining different types of content, such as text, images, audio, and interactives, has been shown to accommodate different learning preferences and increase comprehension. Audio-based scenarios, visual options, and interactive choices support learners in both identifying attack signals and understanding attacker techniques. Research supports the claim that using multiple learning approaches increases cognitive engagement and improves behavioral outcomes in cybersecurity education [8].

Behavioral Change and Adaptive Learning

Recent research emphasizes the importance of influencing user behavior beyond a simple transfer of technical knowledge. Technologies displaying immediate consequences, showing the consequences of hazardous behavior, and guiding proper behavior have been shown to effectively encourage secure behavior. Adaptive learning approaches, taking into account user performance and typical mistakes, greatly enhance learning effectiveness and long-term retention [9].

Current literature reveals that most of the available studies underline the shortcomings of conventional cybersecurity awareness and highlight the benefits of gamification, serious games, and scenario-based learning. Based on these findings, CyberScape introduces immersive simulations, interactive challenges, and real-time feedback for providing an effective and highly practical cybersecurity awareness program that answers the deficiencies found in previous research.

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

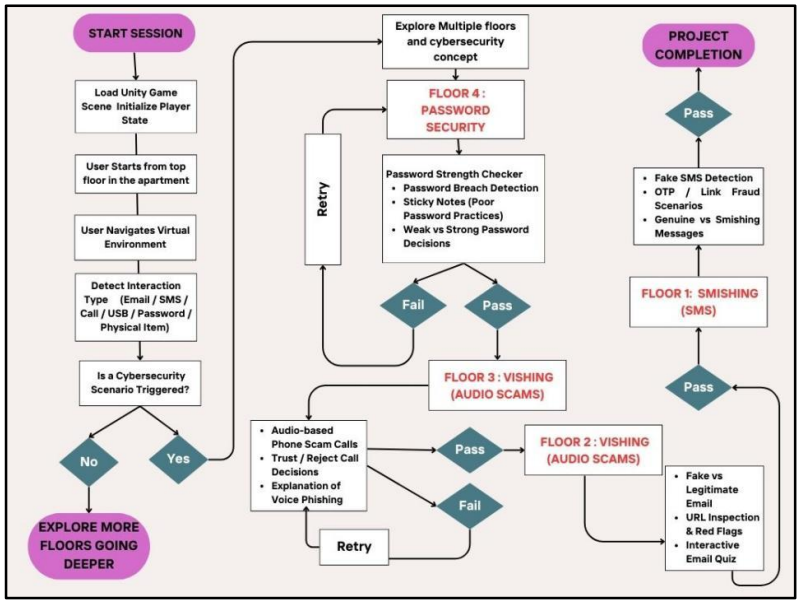

Fig.2: WorkFlow Diagram

Limitations and Future Directions

While immersive and gamified cybersecurity awareness programs present many advantages, there are a series of challenges in the process of their development and integration into practice. First, the need for high computational resources and interaction scenarios required to run concurrently in real time is very high. The systems that are developed using game engines require reasonably good hardware; hence, access on weaker devices will suffer significantly. The creation and maintenance of realistic and up-to-date cybersecurity simulations involve continued commitment to reflect the changing nature of attack vectors.The other big challenge is in measuring long-term learning outcomes and behavioral changes. While gamification successfully generates immediate feedback and engagement, it remains problematic to confirm whether users retain and continue to apply cybersecurity knowledge in real-world scenarios. Moreover, user interaction data for performance evaluation has to be handled very carefully in order to protect ethics, transparency, and user privacy.Future updates could include multiplayer and cooperative learning capabilities, advanced analytics for the assessment of changes in behavior, and the integration of state-of-the-art technologies like virtual reality for more effective engagement. By overcoming these limitations, CyberScape will become a more flexible, scalable, and effective solution to deal with emerging cybersecurity challenges through practical education and outreach programs.

V. APPLICATIONS

Educational Institutions:

CyberScape can be deployed in schools, colleges, and training institutes to interactively teach cybersecurity concepts. The gamified floor-wise structure will allow the students to understand password security, phishing, smishing, and social engineering through practical interactions rather than theoretical teaching.

Corporate Cybersecurity Training:

The integration of CyberScape into employee training programs will enhance the level of cybersecurity awareness and reduce human-related security risks. Simulation of real attack scenarios allows employees to practice recognizing such threats and the corresponding responses, thus reducing further risks associated with data breaches and potential financial losses.

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

Cybersecurity Awareness Platforms:
It can also be used as an awareness tool for the general public to understand common cyber threats. Interactive simulations and real-time feedback enable users to recognize risky behaviors and develop safer online practices within a controlled environment.

Skill Development and Self-Learning:
CyberScape can be used as a self-directed training tool by those looking to learn cybersecurity concepts. The game-like progression and instant feedback will help the learners continue learning the concepts and make cybersecurity education accessible and more interesting for the starters or non-technical users.

VI. FUTURE SCOPE

- Adaptive Learning and AI-Driven Scenarios: Future releases of the CyberScape tool can include the use of AI adaptive learning algorithms which can change the difficulty involved in the scenarios depending on the performance. This will help with adaptive learning.
- Explainable Learning Feedback (XAI Concepts): Use of explanatory mechanisms in feedback will enable users to understand why a certain action was correct or incorrect. This will enable greater user trust and an increased comprehension of concepts related to cybersecurity.
- Multiplayer and Collaborative Learning: CyberScape can also be expanded for multiplayer or team play, where customers work together on cybersecurity issues. This method can represent true organizational settings and improve team and communication techniques.
- Virtual Reality (VR) and Augmented Reality (AR) Integration: The system can also be supplemented with the use of either VR or AR technology for better immersion. This will help users experience cyber-security situations in more real-life setups.
- Behavioral Analytics and Learning Assessment: Advanced analytics can also be incorporated to analyze patterns and trends associated with user behavior decisions. Data will help teachers and organizations determine the effectiveness of learning and areas where additional training is needed.
- Cross-Platform and Mobile Deployment: Extension of CyberScape to mobile and web platforms will ensure easy access and will help users acquire cybersecurity practices anywhere and anytime, especially for awareness and training purposes.
- Expanded Cybersecurity Domains: Future enhancements may involve a range of other cyber-security related topics like ransomware recovery, data privacy laws, cloud security, as well as Internet of Things or IoT Security. Thus, the trend aspect is considered.
- Integration with Academic and Corporate Systems: CyberScape can also integrate well into Learning Management Systems (LMS) as well as Corporate Training platforms for Automated Progress Tracking and massive deployment.

By integrating these improvements, CyberScape has the ability to transform into a full-fledged adaptive and scalable cybersecurity awareness system that meets the challenges of the emerging new age of digital threats.

VII. CONCLUSION

The threats of cybersecurity keep advancing, leveraging human vulnerabilities through elaborate methods, including phishing, smishing, vishing, malware attacks, and social engineering. In real-life situations, users are not sufficiently empowered to recognize and respond to threats through traditional methods of cybersecurity education. This paper presented CyberScape, a comprehensive and immersive gamified cybersecurity awareness system developed for overcoming the limitations of passive learning approaches.The proposed system uses a Unity-based interactive environment to simulate realistic cybersecurity scenarios that involve the active learning of users through direct experience and decision-making. By incorporating scenario-based challenges, rich multimedia elements, and immediate feedback mechanisms, CyberScape serves effectively as the link between theory and practice. Structured progress brings about gradual learning floor-wise, maintaining user engagement and motivation.

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

While the present implementation has strong potential as an educational and awareness tool, there is certainly room for further improvement. In sum, this research underscores the role of experiential and gamified learning in cybersecurity education. Accordingly, CyberScape forms a sound basis for the enhancement of cybersecurity awareness and user behavior, with its contribution toward a safer digital ecosystem. Further research and development regarding game-based learning approaches will, however, become imperative to cope with emerging cyber threats and harden human-centered cybersecurity.

REFERENCES

[1] A. Spatafora, M. Wagemann, C. Sandoval, M. Leisenberg, and C. Vaz de Carvalho, "An educational escape room game to develop cybersecurity skills," Computers, vol. 13, no. 8, p. 205, 2024.
[2] A. Jaffray, C. Finn, and J. R. C. Nurse, "SherLOCKED: A detective-themed serious game for cyber security education," arXiv preprint arXiv:2107.04506, 2021.
[3] T. Srivatanakul, "Designing cybersecurity escape rooms: A gamified approach to undergraduate learning," Journal of Cybersecurity Education, Research and Practice, 2024.
[4] A. K. Gwenhure and F. S. Rahayu, "Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review," International Journal of Serious Games, vol. 11, no. 1, pp. 83–99, 2024.
[5] J.-W. Bullee and L. Koning, "Cybersecurity on the move: Investigating the efficacy of a movable escape room as an educational tool for healthcare employees," in Proc. European Conf. on Games Based Learning (ECGBL), 2024.
[6] D. Pramod, "Gamification in cybersecurity education: A state-of-the-art review and research agenda," Journal of Applied Research in Higher Education, 2024.
[7] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work? A literature review of empirical studies on gamification," in Proc. 47th Hawaii Int. Conf. on System Sciences (HICSS), IEEE, 2014, pp. 3025–3034.
[8] A. McCarthy and J. Wright, "Using escape rooms for cybersecurity education," in Proc. 51st ACM Technical Symp. on Computer Science Education (SIGCSE), ACM, 2020, pp. 701–707.
[9] R. Suryani and P. Asih, "Educational escape room for teaching information security awareness," Journal of Information Systems Education, vol. 32, no. 3, pp. 1–9, 2021.
[10] National Institute of Standards and Technology (NIST), "Cybersecurity framework," NIST, Gaithersburg, MD, USA, 2022. [Online]. Available: https://www.nist.gov/cyberframework