FLAGGED: CYBERSECURITY TRAINING AND AWARENESS SYSTEM THROUGH VIRTUAL REALITY

Haya Alhawas, Noura Althemali, Renad Alkhaldi, Renad Alziyadi, Maali Alabdulhafith

College of Computer Science and Information, Princess Nourah Bint Abdulrahman University, Riyadh City, Saudi Arabia

ABSTRACT

With the persistent rapid growth and sophistication of cyberattack attacks, organizations and individuals have a growing need to prioritize cybersecurity measures. The variety of attacks has posed new challenges and made it difficult to defend against all attacks. The existing traditional training methods are inadequate to keep up with the changing nature of cyberattacks. This project will address the essential problems in cybersecurity training, which are lack of awareness, inadequate customization, and the ineffectiveness of traditional methods, and it will offer a streamlined solution to solve these issues. The metaverse is considered the next evolution of the internet and provides significant innovative solutions for various problems. The metaverse has recently entered the education and training sector as an effective tool to enhance immersive learning experiences. With the objective of leveraging metaverse technologies such as virtual reality (VR) for education, training, and awareness. Flagged aims to develop a comprehensive virtual reality (VR) experience for cybersecurity training and awareness, focusing on phishing attacks. The user will work in the security operations center (SOC) and be responsible for monitoring, investigating, and responding to security incidents, focusing on phishing detection. The environment adapts the gamification and peer instruction (PI) learning methods to ensure collaboration and enhance users' practical skills for achieving the best outcomes.

KEYWORDS

Metaverse, Virtual Reality, Cyber security training, Gamification, Peer Instruction, Cyberattacks

1. INTRODUCTION

In today's digital landscape, with massive global rates of internet consumption by individuals and organizations ranging from academia and government to industrial sectors, the relentless growth and sophistication of cyberattacks have placed organizations and individuals in a constant battle to safeguard their sensitive information and digital assets. Defending against such attacks has gotten more difficult as the diversity of cyberattacks keeps growing. Traditional cybersecurity training techniques are finding it harder to keep up with the constantly changing nature of these attacks, requiring the creation of innovative approaches to this urgent issue.

The significance of robust cybersecurity measures cannot be overstated. It brings us to the meaning of the metaverse. It is a hypothesized iteration of the internet as a single, universal, and immersive virtual world to facilitate utilizing virtual reality (VR) and augmented reality (AR)

David C. Wyld et al. (Eds): NBIoT, MLCL, NMCO, ARIN, CSITA, ISPR, NATAP-2024
pp. 49-66, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.140505

headsets. In nonformal usage, a "metaverse" is a network of 3D virtual worlds focused on social and economic connections. It describes a world of virtuality and reality beyond the real world, built by human beings using digital technology.[1] Moreover, it is a virtual realm that redefines how we interact, learn, and engage with digital environments. A concept that has gained traction in recent years offers a rare chance to transform cybersecurity training. It provides a more realistic and engaged environment for cybersecurity training, empowering those who want to gain experience to protect themselves effectively.

One main area where the metaverse can have a massive impact is combating phishing attacks, which have rapidly increased in recent years. According to [2], the Anti-Phishing Working Group (APWG), the number of phishing attacks detected worldwide reached 241,324 in the first quarter of 2021, marking a 62% increase compared to the same period in 2020. The rise in incidences is partially attributable to these assaults' simple structure. They may be carried out anywhere, not just where the victims are. Phishing attacks are among the most dangerous types that individuals and organizations encounter due to these perks.

The metaverse has enormous potential to alter the nature of cybersecurity training by leveraging its immersive and collaborative spirit. This virtual world offers cybersecurity experts an opportunity to enhance their expertise, abilities, and preparedness in the face of advanced cyberattacks. By recognizing this potential, our project's main objective is to shape the future of cyber defense by integrating the metaverse with cybersecurity training approaches in doing so providing security awareness, education, and technical training. By harnessing the power of the metaverse and merging it with cybersecurity training, we can revolutionize how individuals and organizations defend against cyberattacks.

One approach we will employ is gamification. Gamification is defined as the use of game elements in nongame contexts, which is, in cybersecurity, a strategy that incentivizes people to solve security-related challenges to improve their hands-on technical expertise and collaboration skills. Hacking gamification utilizes game theory and game mechanics not only for entertainment. But also, to enhance the understanding of cybersecurity concepts.[3]. Additionally, we added the peer instruction (PI) learning method, a student-centered approach that encourages active learning and improves decision-making and engagement through peer discussion and feedback.

With the combination of metaverse, gamification, VR-based taring, and peer instruction, we can revolutionize how individuals and organizations protect their digital ecosystems. This comprehensive approach provides a realistic and engaging learning environment that equips participants with practical skills and helps in effectively defending against cyberattacks. By harnessing the power of the metaverse and these innovative training methods, we aim to usher in a new era of cybersecurity that is more dynamic, proactive, and successful in safeguarding sensitive information and digital assets.

2. PROBLEM STATEMENT & SIGNIFICANCE

In the realm of cybersecurity, despite the increasing number of attacks, there is a lack of advanced training programs available. Studies have shown that only 35% of organizations have a comprehensive cybersecurity plan in place, and a mere 25% have implemented all the recommended security controls [4]. These findings highlight the urgent need for organizations to prioritize cybersecurity training and invest in comprehensive security measures to protect themselves effectively against cyber-attacks. This project will address three critical problems in cybersecurity training: the lack of awareness, inadequate customization, and the ineffectiveness of traditional learning methods.

Firstly, the lack of awareness is a significant issue; many organizations and individuals still lack adequate cybersecurity awareness, making it easier for attackers to succeed. Information security awareness gives the user more understanding of the importance of the best practices [5] .A study conducted by [6] in Saudi Arabia, involving participants from all regions, showed that the general findings indicate a low level of awareness concerning cybersecurity and information security, with only 61% awareness achieved. The result emphasizes the importance of raising awareness to its maximum potential. Several factors contribute to the lack of cybersecurity awareness. One factor is some organizations are not focusing on the insider attacks that originate from within their domain, typically involving employees, contractors, or other trusted individuals. Employees are the front line of defense of any organization for protecting the network as well as the biggest threat [5]. Managers and employees share responsibility in knowing the consequences of cyber-attack risks.

Secondly, inadequate customization, according to the Verizon DBIR report [7], Ransomware was the most common type of attack, accounting for 24% of all breaches, followed by Phishing, Malware, Denial-of-service (DoS) attacks, and Data breaches. Due to the variety of attacks, a critical inadequacy exists in the cybersecurity training solutions presented in the market due to a lack of customizable scenarios that cater to specific types of cyberattacks. A one-size-fits-all security training system is not as effective as a customizable system, which allows organizations to tailor it to their specific threats and vulnerabilities. The increasing risk of cyberattacks on organizations makes them more vulnerable to cyberattacks. This problem can result in resource wastage, such as budget and employee time. Organizations should train their employees on how to defend against these attacks effectively. Furthermore, with the rapid growth of new and advanced cyber-attacks, every cybersecurity training system should be able to adapt to changes without replacing the whole system to fit a new type of attack.

Thirdly, the ineffectiveness of traditional learning methods. These methods within the cybersecurity domain are on the verge of becoming outdated. Sandboxes, antivirus controls, secure email, and other standard technologies were designed to protect networks from direct attackers [6]. To deal with the new phishing assaults that target vulnerable employees, new teaching methods are required [7]. As outlined in [8], the job market demands cybersecurity professionals who can turn their expertise into real-world solutions. Traditional methods became ineffective as they primarily rely on theoretical concepts and principles, preventing cybersecurity professionals from applying their knowledge in real-world scenarios. Also, the current challenge in cybersecurity training systems lies in the lack of collaboration applications. Cybersecurity requires teamwork to achieve collective outcomes, given the complexity of cybersecurity surpasses the cognitive ability of individuals. Traditional methods often lack motivation and do not foster group work. Most employees feel unengaged in text-heavy training programs because it doesn't relate to their real-life work. Which makes it difficult for them to learn and remember the steps they must follow when an attack occurs. Caputo et al. highlighted that employees contine to react negatively to phishing attacks, even when organizations implement traditional training methods. Regardless of how much they spend on training, they may still click on the links [9]. Here comes the importance of using simulations and advanced training systems that provide practical hands-on experiences and enhance teamwork skills, ensuring they are well-prepared for future attacks.

3. PROPOSED SOLUTION

Considering the numerous challenges that face cybersecurity training systems, it has become essential to invent a comprehensive solution that limits these problems to aim at effectively mitigating cyberattacks. Recently, Metaverse has entered the training field and changed the whole concept. For its high capabilities, it provides a more engaging and realistic training

experience for individuals and organizations. To resolve these challenges, we developed a Metaverse environment that adapts the VR technology, providing learners with a secure and controlled space where trainees can make mistakes without putting actual systems at risk. The immersive experience simulates a phishing attack scenario, placing the user inside a Security Operations Center (SOC) as a cybersecurity analyst responsible for tackling and detecting the phishing attack. Experiencing cyberattack scenarios can influence learners' behavior, making them more cautious in handling emails and online activities.

To address the lack of awareness, our Metaverse-based solution faces this challenge by immersing learners in real-world cyberattack scenarios. The primary goal of spreading cybersecurity awareness is to empower individuals and organizations with the knowledge and skills needed to safeguard their digital assets and work environment against cyberattacks. Phishing attacks are common in organizations and are mostly used to assess the level of employee awareness. Phishing training is a significant example of cybersecurity awareness. An investigation of the phishing threat on human behavior is conducted by Nalin et al. in [5]using a mobile game prototype. The result shows a marked improvement in participants' behavior in avoiding phishing threats. Utilizing advanced training systems enables employees to acquire a comprehensive understanding and the confidence needed to respond to real-life cyberattacks.

We recognized the need for customizable cybersecurity training systems that allow organizations to tailor their training programs to specific needs and adapt to emerging cyber-attacks, helping in improving the effectiveness of the training and reducing the risk of cyberattacks. Customized training systems raise employee attention directly by relating to their roles and demonstrating the specific types of cyberattacks they may face. Also, these systems benefit all employees, regardless of their cybersecurity knowledge and expertise. Adapting a customized training system is an investment choice because it encourages employee familiarity and eliminates organizations from handling numerous systems to streamline the training effort. As a result, it improves the overall security posture of the organization.

To address the inefficiency of traditional learning methods, we integrated gamification and PI as primary learning approaches. Virtual worlds are primarily used for gaming [10]. Gamification is defined as the use of game elements in nongame contexts (Deterding et al. 2011). The belief about gamification effectiveness is taken from the association with the game experience, given its characteristics of being fun and intrinsically motivating. The goal of gamified systems in cybersecurity education and training is to change a person’s behavior toward a desirable outcome [3]. In a study made by [11], after experimenting with gamification in companies’ work environments, there has been a 50% increase in the ability to recognize phishing attempts and an 82% increase in the rate of reporting such incidents. The second approach is PI. It is a well-defined teaching protocol designed to enhance engagement between learners. It involves conceptual multiple-choice questions (MCQ) and group discussion activities [12]. PI has proven its effectiveness in cybersecurity education, and it can be particularly well-suited for VR-based training. It can be implemented by asking the trainees questions as they go through the given scenario. These questions could include what they should do next or ask about security concepts. Since Metaverse is a collaborative environment, Trainees can discuss their answers as a group once they have the chance. Based on student surveys, 77% of them found that group discussions with their classmates helped them understand security concepts, and 70% of them would recommend PI to other.

4. RELATED WORK

4.1. Work & Research Methodology

CBL stands for Challenge-based learning [13]. CBL is a learning model that focuses on developing the learner's ability to perform specific tasks. It is a cyclical model consisting of three main phases: Engage, investigate, and act.

We implemented this pedagogical approach, starting with identifying the big idea, asking guiding questions, looking for answers, gaining in-depth subject area knowledge, identifying, and solving challenges, developing critical thinking and research skills, and learning how to learn. The CBL framework emerged from the Apple Classrooms of Tomorrow—Today" (ACOT2) project, a collaborative effort with the education community to identify the essential design principles for the 21st-century high school by focusing on the relationships that matter most: those between students, teachers, and curriculum [14].The project aims to create a learning environment appropriate for this generation of high school students and satisfy their needs [14].

The CBL is flexible and customizable and can be implemented in various subjects. The Challenge Learning Framework includes three interconnected phases: Engage, Investigate, and Act. Each phase contains required tasks to move to the next one. After pursuing this framework, we successfully identified the problem statement and reached the optimal solution. The main idea of the project is cybersecurity. To address all four problems comprehensively, we posed four fundamental questions (what, who, whom, when) to ensure a thorough understanding and access to the most relevant articles for our literature review, thus enhancing the quality of our research outcomes, see Table 1. Furthermore, after conducting our research, we discovered a significant relationship between the last two problems, prompting us to combine them for a more coherent analysis.

4.1.1. CBL Advantages

We identified CBL as the optimal approach relative to other approaches to conduct our research due to its enhanced ecological validity, focusing on real-world problems and contexts. Providing insights beyond traditional research methods conducted in artificial environments [15] while relying on critical thinking, problem-solving, collaboration, and communication aspects. This aspect is of value when designing a virtual reality system for training purposes [16]. Another reason for choosing CBL as our research methodology is to promote interdisciplinary collaboration, involving researchers, educators, and practitioners from different disciplines, fostering the development of comprehensive and innovative solutions for our system evaluation and enhancement [17]. Furthermore, the CBL approach allows for continuous evaluation and improvement of research methods and our system throughout the research process. This iterative process makes it easier to identify and address any issues early, ensuring that the research leads to meaningful and impactful results.

Table 1: CBL guiding questions during the research journey

		Guiding Questions			
No.	Problem	Who	What	When	Where
P1	lack of awareness	who needs the awareness?	What causes the lack of awareness?	When awareness needs to be raised?	Where are the gaps in awareness of most pronouns? Where should cybersecurity training should be delivered?
P2	inadequate customization	Who will benefit the most from having a customizable system?	What are the negatives of not having a customizable system? What are the most common threats or cyber-attacks that have been reported in our industry?	When is customizable system are effective?	Where customizable are used the most?
P3	ineffectiveness of traditional learning methods	Who would need the interactive tools?	What method of learning should these interactive tools adapt?	When should these interactive tools be most needed?	Where should interactive tools be implemented?
P4	Absence of Collaboration	Who will need a collaborative system?	What are the benefits of having a collaborative system?	When should collaboration be considered in cyber security?	Where is collaboration, most needed in cyber security?

4.2. The Role of Metaverse in Cybersecurity Training

Given the alarming growth in cyberattacks, traditional Cybersecurity training is often outdated and ineffective. The IBM (2022) report declares that in the current year, 25% of security breaches in industrial organizations occurred due to human errors [18]. This study indicates that traditional training methods are not refining skills to handle real situations. The COVID-19 pandemic accelerated online learning and training adoption, making technology an essential part of education and workforce development. One newly introduced technology is the metaverse, which gives trainees an immersive experience in a three-dimensional environment. Participants can practice training scenarios in realistic settings to gain hands-on experience (Park and Kim, 2022). With the popularity of the metaverse, research papers are beginning to shed light on the potential benefits of integrating the metaverse with cybersecurity training.

This literature review highlights how the metaverse can improve training outcomes, as we found throughout [18, 19]. The metaverse holds significant potential to revolutionize the e-learning industry, called Meta-education [19]. In [18], the prospect that the metaverse could have for improving training and development was discussed; similarly, in [20], the integration of the metaverse was emphasized, and the potential it has to revolutionize traditional training approaches and its impact on enhancing employee experience, communication, knowledge sharing, job satisfaction, and other positive outcomes (Hajjami and S. Park) due to it being an

innovative tool that is used to create personalized training environments that increase employee performance.

All studies [18, 19, 20, 21] explore the impact of using the metaverse, which has spread across various fields, including education and training, such as virtual classrooms, industrial, aircraft, maritime, and military training. Due to all the features that VR-based training provides; it is considered the most effective technique for training. Based on the author's research [20], scholars indicated that the metaverse increases motivation and facilitates learning. A recent study examined the effect of VR metaverse training on learning soft skills with 12 US managers (PwC, 2021). Learning soft skills through VR was four times faster than classroom and online-based training. In addition, the metaverse supports customizing learning experiences based on learners' needs. Also, the paper summarized 14 cases based on the type of training using metaverse. Such as designing a Ship safety training program and BMW Assembly line training using AR, where they saved time, avoided safety accidents, and reduced prototype costs. The metaverse proved its efficiency through multiple applications, making it an advanced tool for training and education.

Where [19] found that the objective of exploring metaverse technology in the education and training sector is to address the challenges and opportunities it presents. The metaverse offers features, including a deep immersion experience, an embodied social network, group-free creation, a social civilization ecology, and virtual and real-life integration. (W. Shao) believes that the metaverse can address the limitations of MOOCs, which are free online courses that provide high-quality education. However, their completion rates could be higher due to the use of the 2D format. Metaverse allows trainees and instructors to assemble in a virtual environment regardless of their real-world location.

Furthermore, the integration of metaverse [18, 19, 21] shares similarities in the emphasis on the VR aspect. VR-based Cybersecurity Training is the new form of game-based training [18]. It employs gamification and multiuser learning [18, 19]. Meta-education was highlighted as it enables employees to collaborate and improve their teamwork skills to share experiences and overcome challenges [19]. VR-based Cybersecurity Training provides an immersive and realistic interaction experience for employees, besides entertainment and engagement. VR-based Cybersecurity Training includes three-dimensional space, advanced visual effects, and realistic simulations of cyberattacks. VR systems allow users to interact with objects inside the virtual environment. By emerging real-life scenarios with VR, employees can develop practical skills, improve decision-making abilities, and enhance their understanding of complex cybersecurity concepts. VR-based training is a superior cybersecurity approach that significantly affects knowledge retention [18]. Technologies such as Extended Reality (XR) and the Internet of Everything (IoE) play influential roles in educational services in future metaverses [21].

As mentioned in [18, 20], both papers share similarities and differences in their focus on the fact that current training systems could be more flexible as they assume all employees have the same knowledge and skill level. Due to boredom and lack of engagement, lecture-based, text-based, and video-based training could be more effective. Lecture-based and text-based training approaches exhibit rigidity, need to adapt learner requirements, and often need more relevant cybersecurity training content. Web-based failed to deliver a training experience close to reality and provide interaction and engagement [20]. Despite its online nature, it refuses engagement and interactivity. Simulation training positively impacts trainees due to its applicability in different fields. In cybersecurity, professionals can predict different types of attacks. The metaverse addresses these limitations by providing a realistic and blended physical-virtual environment. Moreover, the metaverse is a secure environment for developing hands-on experiences that mitigate human and material risks during the training [20]. With emerging technologies like VR and AR [18], trainees can join the experience using personal avatars and practice training

scenarios in realistic settings that provide hands-on experience. (Park and Kim, 2022). Which enhances connectivity and interaction among trainees.

Moreover, [6,7] [22, 23] focuses on the ineffectiveness of current cybersecurity programs and the need to provide a strong background. This leads to obtaining certifications as a favored source of cybersecurity education, such as CompTIA. Recently, VR systems are replacing expensive and without having to create a physical prototype. However, for a better training experience, the VR environment should support free movement. VR-based training can overcome all the obstacles to movement challenges in the simulation Systems. Based on the [23] survey findings, the participants' feedback was collected using questionnaires. The system testing has two phases with a week-long gap. In the first test, 90% of the participants remembered the data center's physical security layers and the procedure of fixing a node with a broken RAM. In the second test, 80% of the participants still remembered the details of the data center security checkpoints and the procedure for replacing hardware in the node, which shows the VR-based training system's positive impact on the students. Metaverse can revolutionize the training sector [23]. Both (A. K. Upadhyay) (K. Khandelwal) cited that several reports highlighted that organizations that adopt VR training will have rapid growth in the future. Organizations will adopt AR and VR for training and work meetings. Also, experts believe that the cost of access to 3D training solutions will decrease with time and development, resulting in greater adoption of metaverse-based training [22].

Overall, the findings of this literature review showed that the metaverse presents a transformative opportunity for cybersecurity training. By leveraging its immersive, interactive, and customizable nature, the metaverse can empower individuals and organizations to develop the skills necessary to combat evolving cyber threats and safeguard the digital world.

4.3. VR-Based Cybersecurity Training

When delving into VR-based training, it is crucial to grasp its variety in diverse fields of study. In our scenario, our focus is directed towards the cybersecurity domain. In this literature review, we explore seven studies focused on VR in the context of cybersecurity training. These studies collectively address various aspects of VR technology's application to cybersecurity education, training, and engagement. The central themes and topics explored within these papers revolve around enhancing cybersecurity through VR technologies, and the key questions and issues they aim to tackle encompass the efficacy of VR-based training, the development of VR cybersecurity training frameworks, and the identification of cybersecurity challenges in VR environments.

Our research leads us to the fact that all [24, 25, 26, 27, 23, 28, 29] have a shared focus on VR technology training and the unlimited possibilities that come with it more specifically, the cybersecurity domain. But when delving further into these papers, we can see that articles [24, 25, 27, 23] share a focus on the implementation aspect of VR technologies in cybersecurity education and training and the exploring potential benefits of these technologies in improving distance and remote education, enhancing engagement and retention, and providing realistic simulations for cybersecurity training focusing on implementing ways on providing users engaging scenarios to teach cybersecurity concepts and provide high-immersion learning experiences while highlighting the potential advantages of utilizing a range of immersive technologies.

However, article [27] discusses the use of immersive learning and VR technology for teaching cybersecurity concepts. It highlights the importance of incorporating physical aspects of cybersecurity into training programs and addresses the limitations of existing cybersecurity

programs in this area. Unlike in article [23], the focus is on using VR to enforce cybersecurity principles.

Whereas [26, 28, 29] research is focused on the application of VR in specific training scenarios even though the application of each system is different, they do share the goal of effectiveness in improving cybersecurity knowledge and skills and further exploring the immersive and interactive nature of VR training providing results that show that using a VR environment can be a promising modality for providing cybersecurity training.

The findings of these papers shed light on the potential of VR to enhance cybersecurity training. By examining these studies, we aim to identify the key areas of consensus and divergence within the literature. Ultimately, our review underscores the promising outlook for VR-based cybersecurity training as a viable alternative to traditional methods and suggests possible directions for further research in this evolving field.

4.4. Gamification in Cybersecurity

Gamification is commonly defined as integrating game elements and mechanics into non-game contexts to enhance engagement, motivation, and participation. It incorporates points, levels, badges, leaderboards, challenges, rewards, and feedback to make tasks or activities more enjoyable and interactive [30, 31, 32, 33, 34, 35, 36]. Based on [34], a survey of 200 training professionals revealed that 70% had implemented gamification in their programs. Popular techniques included badges (82%), leaderboards (78%), and points (76%). Respondents reported positive effects on employee engagement (84%), motivation (82%), and learning outcomes (79%). However, interpretations and applications of gamification can vary significantly among studies. Several studies emphasize gamification in education, while others may explore its implementation in corporate training, employee development, or cognitive training. Furthermore, the articles may vary regarding the methodologies used to study gamification and the contexts in which it is examined.

Based on [31, 32], the authors assert that their respective articles share a common topic of gamification in cybersecurity. Collectively, they explore the application and benefits of gamification techniques in cybersecurity education, training, and awareness. They highlight the potential of gamification to enhance engagement, motivation, learning outcomes, and behavior related to cybersecurity practices. Additionally, the articles discuss the use of gamified approaches in creating interactive and immersive learning experiences, simulating real-world cyber threats, and promoting active participation in cybersecurity training programs. However, the articles differ in focus, methodologies, target audiences, objectives, and gamification techniques. Some articles review the empirical literature on gamification in education and learning, while others evaluate its effectiveness in corporate training, employee development, or computerized cognitive training. Furthermore, specific articles address the successful gamification of cybersecurity training or techniques for raising cybersecurity awareness.

Both [33, 34] recognize the potential of incorporating game elements and mechanics to enhance engagement, motivation, and learning outcomes. However, they differ in their specific focuses. (J. Majuri et al., 2012) (J. Majuri and J. Hamari, 2017) They mentioned the review of the empirical literature on gamification in education, examining its effectiveness across various educational levels and subjects. (M. B. Armstrong et al.; R. N. Landers) mentioned examining gamification in employee training and development, exploring its role in improving engagement and skill acquisition within organizational contexts. Both studies [35, 36] explore the impact of gamification in training but differ in their specific contexts. They both employ a meta-analysis approach to analyze the effectiveness of gamified elements such as rewards and challenges. The

studies find positive effects of gamification, including increased motivation, engagement, and learning performance. However, as mentioned in in [35], it focuses on gamification in corporate training, while the second [36] examines gamification in computerized cognitive training. The measurement of outcomes and participant characteristics also differ between the articles.

In general, these systems recognize the need for innovative approaches and emphasize the limitations of traditional methods. They highlight the importance of customization and immersive experiences to enhance learning outcomes. Specifically, integrating VR experiences is emphasized as a powerful tool to create realistic and engaging learning environments. Additionally, the potential of gamification and collaboration is emphasized, suggesting using game elements and mechanics to increase user engagement and motivation. However, it's important to note that while the articles may not directly address the cybersecurity domain, the underlying principles and strategies discussed can be applied to develop a comprehensive VR system for cybersecurity training. By leveraging these insights, you can create a tailored system that addresses the challenges in cybersecurity training and enhances users' practical skills in phishing detection.

4.5. Peer Instruction (PI) Learning Approach

Peer Instruction (PI) learning approach is a teaching methodology that encourages active learning and collaboration among students [37, 38, 39, 40, 41, 42, 43]. It involves students learning from and teaching each other under the guidance of an instructor. The articles explore how PI can enhance learning outcomes and student engagement in cybersecurity education. They investigate its effectiveness, impact on learners with different cognitive styles, and use in developing tailored materials, workshops, and curricula. Some articles also examine the effectiveness of peer mentoring, which is a form of PI, in computing courses related to cybersecurity and data analytics. Overall, these articles contribute to a deeper understanding of how PI can be effectively applied in various aspects of cybersecurity education.

Both studies [38, 39] share similarities and differences in their focus and methodology. Both articles explore the application of PI in cybersecurity education, aiming to enhance learning outcomes and student engagement through collaborative learning and active participation. However, as mentioned in [38], it specifically examines the impact of PI on learners with different cognitive styles in a VR learning environment. At the same time, the second [39] focuses on measuring the effectiveness of peer mentoring (a form of PI) in data analytics for cybersecurity.

The studies [40, 41] share similarities and differences in focusing on the PI learning approach in cybersecurity education. In The [40] emphasizes creating PI material tailored for a cybersecurity curriculum, while the second [41] explores the broader application of PI in cybersecurity and data privacy. These articles provide valuable insights into utilizing PI in different aspects of cybersecurity education. Both [42, 43] are related to the PI learning approach. In [42], it explores the integration of serious games and PI in a digital forensics workshop. (L. Engelbrecht et al.,2020; G. Pernul,2020) They mentioned examining the broader application of PI in cybersecurity education. Both articles emphasize the advantages of using PI to enhance learning outcomes and engagement in their respective contexts.

In general, we align with the articles in addressing challenges in cybersecurity training and proposing innovative solutions. We both recognize the limitations of traditional methods and the need for customized approaches. However, these unique technological approaches offer a more immersive and engaging cybersecurity training experience.

5. PROPOSED SYSTEM & SIMILAR SYSTEMS COMPARISON

Our suggested approach focuses on creating a dynamic and captivating learning environment through metaverse-based VR technology. Traditional training often relies on passive learning tools, such as standard guide techniques, which may not provide an immersive and interactive learning experience [44]. Additionally, traditional training methods may not effectively engage learners or promote long-term retention of knowledge [27]. Flagged aims to solve the shortcomings of conventional training techniques, including inadequate customization, ineffectiveness, and lack of awareness. The key components of our proposed system include:

A. Virtual Reality (VR) Experience:

The system offers an all-encompassing VR experience for cybersecurity training, with a specific focus on phishing attacks. Users will immerse themselves in a virtual environment that simulates a SOC while assuming the role of a security analyst. Their responsibilities will include monitoring, investigating, and responding to security incidents, with a particular emphasis on detecting phishing attempts. The VR environment will faithfully replicate real-life scenarios and challenges, ensuring a realistic and engaging training experience.

B. Gamification:

To enhance user engagement and motivation, Flagged will incorporate gamification elements into the training process. Users will be presented with security-related challenges and tasks within the VR environment, enhancing their end performance percentage as they progress. Gamification techniques will be employed to create a competitive and immersive learning experience. This approach aims to increase user participation, knowledge retention, and practical skill development.

C. Peer Instruction (PI):

To promote user participation and active learning, Flagged will incorporate PI learning methodology. Users will have the chance to cooperate to solve security problems by exchanging knowledge and ideas through answering MCQ questions and peer discussion. This collaborative approach fosters communication, critical thinking, and decision-making abilities in addition to improving the effectiveness of learning.

D. Customization and Adaptation:

Recognizing the significance of customization in cyber security training, Flagged would make it possible for organizations to have customized training scenarios according to their particular needs. Users can choose specific training modules and focus on areas of interest or weakness. Flagged will dynamically adjust the training content to provide a personalized and optimized learning journey.

By leveraging the power of Metaverse, VR, gamification, and PI, our proposed system aims to revolutionize cybersecurity training. It offers a realistic, immersive, and adaptable learning environment that improves users' practical abilities and gets them ready for combating cyberattacks, especially phishing attacks, with efficiency. The system's creative methodology overcomes the drawbacks of conventional training techniques and gives organizations and individuals the skills and information they need to prioritize cyber security measures against changing attacks.

Table 2. Comparative analysis of cybersecurity training systems

	Our Proposed System	Onebonsai Cybersecurity Awareness	VRE Cybersecurity Training and Assessment	Immersive Labs	Active shooter response training By STIRVR
VR-based system	✓	✓	✓	✗	✗
Target Organizations	✓	✓	✓	✓	✓
Ease of Installation	✓	✓	✓	✓	✓
Enhance Collaboration	✓	✗	✓	✓	✓
Customization feature	✓	✓	✓	✗	✓
Adopt Learning approaches	✓	✗	✗	✗	✗
Scenario-Based System	✓	✓	✗	✓	✓
Usability	✓	✓	✓	✓	✓
Scalability	✓	✓	✓	✓	✗
Analytics	✓	✓	✗	✗	✗

6. REQUIREMENTS ANALYSIS

6.1. Use Case Diagram

Figure 1. illustrates the Use-case diagram to give a comprehensive overview of the system functionality and show the interaction between the system and its actors. The actor represents the user who performs the 11 tasks, known as cases. (1) Users can start the experience once they follow the room creation or joining process (2) Users can read the system user guide after running the experience, which is known as onboarding. It introduces the user to the system and guides them to interact within it (3) Users must enter their names before joining training rooms for identification purposes. (4) Users can create a new room on the server to initial a new training module. (5) Users can join an existing room by choosing from the available room list or manually entering the room ID. (6) To complete the training module, users must detect the attack. The core mechanism of the system is private because it shows the description of the system operation to which users have no access. It relies on generating tasks for users on specific attack scenarios. These tasks are performed by answering MCQ questions. (7) Users can send and receive data by communicating with other users, submitting answers, and receiving their final scores. (8) Users collaborate to solve the challenge and achieve the training goal. (9) By the end of the experience, users will receive a work performance chart that breaks down the questions answered correctly and incorrectly to provide an overall score to outline weaknesses and strengths areas. Besides the chart, a leaderboard ranks the user's places based on their performance against others who have completed the training within the room, further enhancing the competitive and collaborative aspects of the learning experience. (10) Users can exit the experience at any time. However, they

cannot pause and resume it later due to its real-time nature. (11) The multiplayer network offers multiplayer services and manages the sessions, ensuring its reliability and efficiency to provide users with the best engagement experience. Also, it controls how data are sent and received between the users.

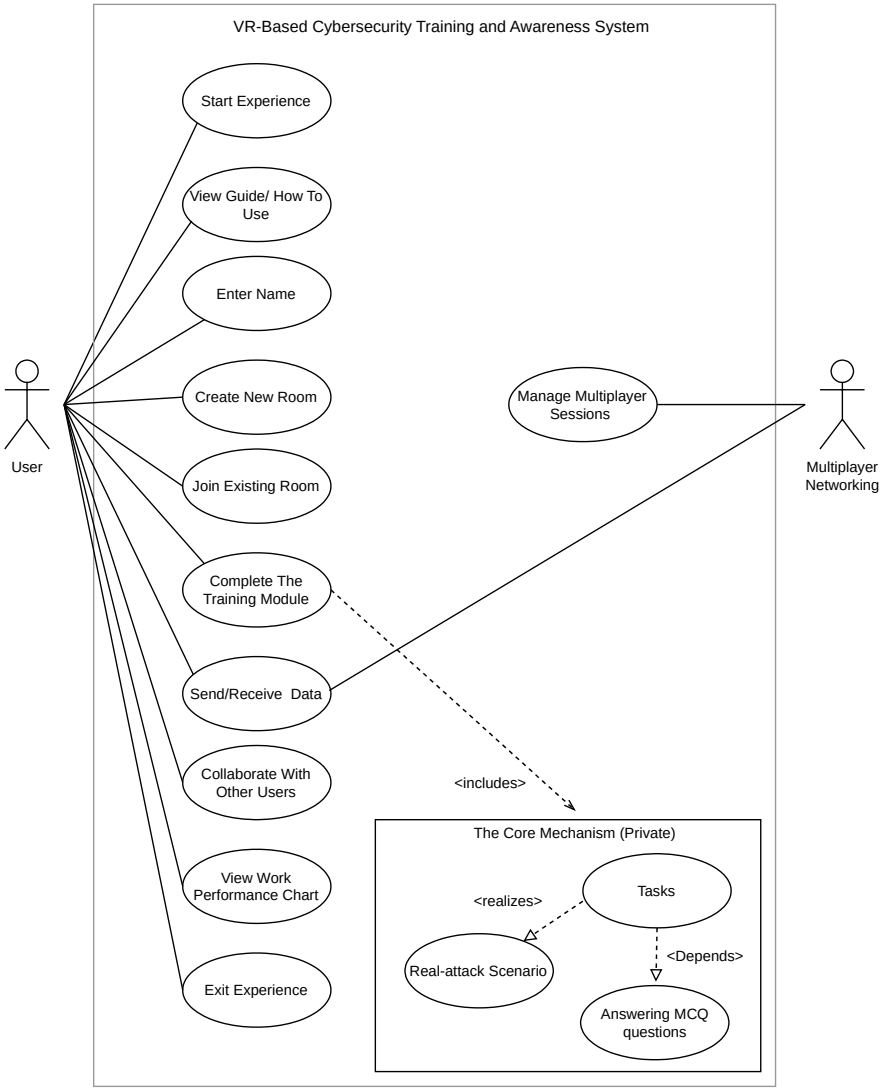

Figure 1. A graphical depiction of the interactions between a system and its users

6.2. VR-based Cybersecurity Training and Awareness System Workflow

Figure 2. illustrates a flowchart that visualizes the process step-by-step that the user takes to complete tasks or goals within the system. The user initiation involves entering the system and providing their names. Then, users can either read the guide/how-to screen or not. Subsequently, users encounter a decision point, deciding whether to join an existing room from the available rooms list or create a new one. Joining an existing one offers two options—entering the room ID or selecting from the list. Creating a new room necessitates naming it. Once all users have successfully joined a room, the training module initiates. The training module follows the system's core mechanism, displaying tasks based on the attack scenario. These tasks are MSQ questions to test the user's knowledge. The system will continuously generate questions based on

users' previous answers for a more realistic scenario until an attack is detected. The attack detection is confirmed if the user answers the questions correctly, which indicates their ability to deal with the attack. After the training module is completed, users will receive a detailed work performance chart. Also, a leaderboard is integrated, ranking users based on their performance within the training experience. Finally, the entire experience concludes, providing users with a comprehensive understanding of the attack's nature and the consequences.

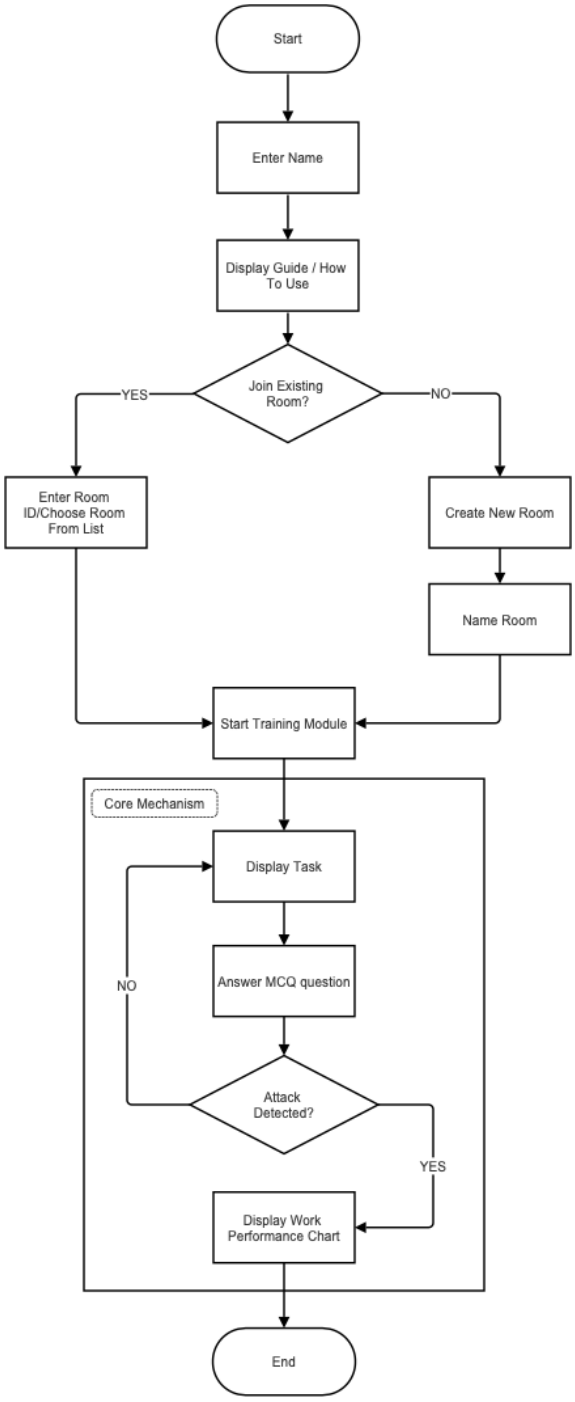

Figure 2. The process of VR-based cybersecurity training and awareness system

7. SYSTEM ARCHITECTURE

Figure 3. illustrates the proposed system's architectural design. We utilized the four-tier architecture, which divides the system into four layers: presentation, application, business logic, and data. This architecture is known for its flexibility and facilitates the system implementation. The four-tier architecture helps developers to understand the system's structure and functionality more comprehensively. It defines the responsibilities of each layer and how it they interact with each other to achieve the system overall functionality.

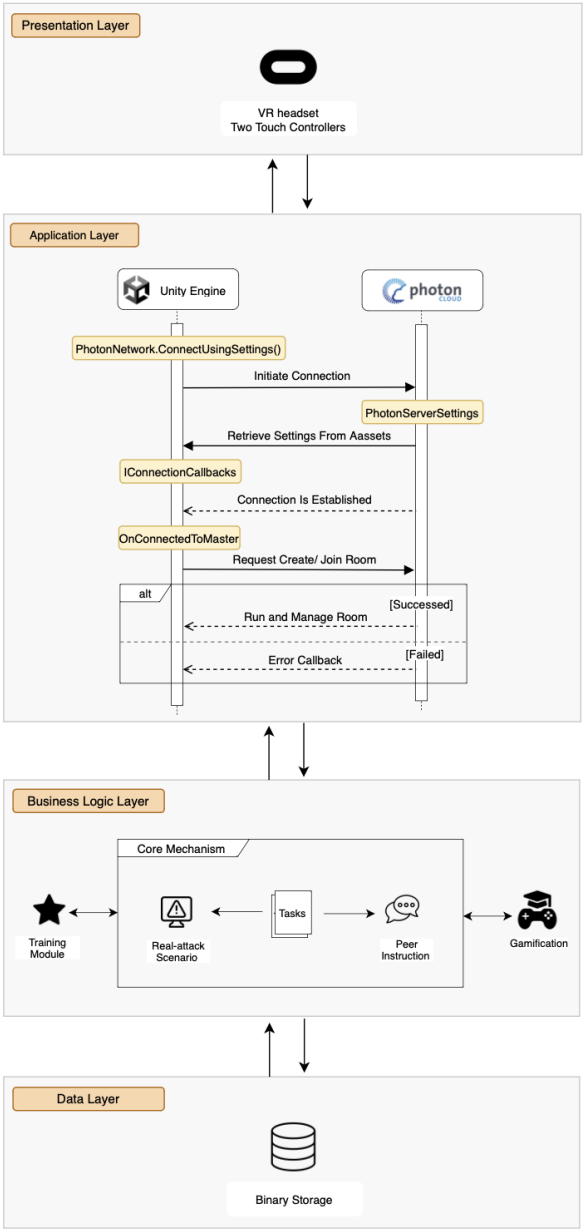

Figure 3. VR-based cybersecurity training and awareness system architecture

A. Presentation Layer :

The presentation layer contains either the software or hardware components that the user uses to interact within the system and receive data from the user. In Figure 7. the presentation layer includes the Meta Quest VR headset and Two Touch Controllers.

B. Application Layer:

The application layer plays a crucial role in a system's architecture by serving as a bridge between the presentation layer and the business logic layer. The application layer shows the core requirements of system implementation, contains the core functionalities, integrates third-party services, and executes complex algorithms. Our system utilizes the Unity engine for developing and designing, while Photon Cloud provides the multiplayer service. Moreover, the presentation layer illustrates the connection between Unity and Photon. Unity uses C# scripts to set up Photon Unity Networking (PUN). (1) After importing PUN into the project, call PhotonNetwork.ConnectUsingSettings() will establish the connection. (2) PUN Wizard will display a popup window for registration and import the PhotonServerSettings file to the project to store a configuration. (3) PUN uses callbacks to notify the developer when the connection is established. (4) OnConnectedToMaster is used for joining and creating rooms to start a session. (5) If the user requests to join an existing room, then the Photon Cloud servers check for room availability. If the room exists, then the user joins. Otherwise, the error callback function is called. (6) If the user creates a new room, it will be created unless errors are encountered such as the room already exists or calls. However, Photon is responsible for managing the multiplayer sessions and communication efficiency.

C. Business Logic Layer:

The business logic layer presents the core functionality of the system. It executes the essential processes and operations that define the application's purpose. Our system core mechanism adapts two main approaches: gamification and PI. The business logic illustrates how these approaches are integrated within the system. The training module relies on the core mechanism, including the tasks generated utilizing real-attack scenarios, and depends on PI for the MCQ questions. Additionally, gamification is incorporated into the system to enhance engagement and achieve optimal learning outcomes.

D. Data layer:

The data layer is responsible for storing and retrieving data using a database management system (DBMS) or a file system. Binary storage refers to how to save and load data in a binary format. Unity provides various ways to perform binary storage, often involving serialization and deserialization of data. Binary storage is valuable for performing tasks such as saving and loading game progress, configuration settings, or custom data structures.

8. CONCLUSION

The increasing number of attacks has highlighted the urgent need for an advanced training system. We have learned that using XR technologies, including Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) can contribute to training employees with different levels of expertise in a much more engaging and motivational way. We have also benefited from the research and insights of experts in the field, indicating that the Metaverse holds a high potential to serve as a tool for advancing various fields. Further, the Metaverse offers innovative solutions for immersive learning experiences, interactive simulations, and collaborative environments,

making it invaluable in shaping the future of education, training, and beyond. This research paper discussed our proposed solution for developing a Metaverse environment for cybersecurity training and awareness. We highlighted the critical problems in cybersecurity training: the lack of awareness, inadequate customization, and the ineffectiveness of traditional learning methods, tackling each problem systematically. We enhance the training experience by leveraging VR technology with gamification and peer instruction approaches. We demonstrated how these approaches contribute to the system's overall effectiveness. This research paper helps researchers, developers, and anyone interested in using Metaverse and its technologies for enhancing education and training. It aims to provide an understanding of the opportunities in the field.

ACKNOWLEDGEMENTS

We would like to thank Eng. Muhammad Alagil and Nora Alagil for their support and generous grant in sponsoring our participation in this conference (Grant No.1). Our gratitude also goes to Princess Nourah University for facilitating the process of participation.

REFERENCES

[1] J. Wu, K. Lin, Z. Zheng, Huang, H and D. Lin, "Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities," 2023.
[2] "Phishing Activity Trends Report 4th Quarter 2022, APWG Unifying the Global Response To Cybercrime Activity," 2022.
[3] F. Inocencio, "Using Gamification in Education: A Systematic Literature Review," San Francisco, CA, USA, 2018.
[4] H. Ruoslahti, J. Coburn, A. Trent and I. Tikanmäki, "Cyber Skills Gaps : A Systematic Review of the Academic Literature," no. 2, pp. 33-45, 2021.
[5] H. Al-Mohannadi, I. Awan, J. Al Hamar and A. Sanda Mu, "Understanding Awareness of Cyber Security Threat among IT Employees," 2018.
[6] M. Alsharif, S. Mishra and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," 2021.
[7] Verizon, "Data Breach Investigations Report (DBIR) by Verizon," 2022.
[8] J. Sigholm, G. Falco and A. Viswanathan, "Enhancing Cybersecurity Education through High-Fidelity Live Exercises (HiFLiX)," Hawaii, 2019.
[9] D. Caputo, S. Pfleeger, J. Freeman and M. Johnson, "Going Spear Phishing: Exploring Embedded Training and Awareness," vol. 12, p. 28–38, 2014.
[10] P. Onu, A. Pradhan and C. Mbohwa, "Potential to use metaverse for future teaching and learning," 2023.
[11] C. Bedell, "How Gamification Can Improve Employee Cybersecurity Compliance," vol. 21, pp. 37-51, 2019.
[12] P. Deshpande, C. B. Lee and I. Ahmed, "Evaluation of Peer Instruction for Cybersecurity Education," 2019.
[13] "Challenge Based Learning provides an efficient and effective framework for learning while solving real-world Challenges.," [Online]. Available: https://www.challengebasedlearning.org/about/. [Accessed 1 11 2023].
[14] "Apple Classrooms of Tomorrow—Today," 2008.
[15] T. Parsons, "Virtual Reality for Enhanced Ecological Validity and Experimental Control in the Clinical, Affective and Social Neurosciences," vol. 9, 2015.
[16] M. Qian and K. Clark, "Game-based Learning and 21st century skills: A review of recent research," vol. 63, pp. 50-58, 2016.
[17] "Open Science for the 21st Century," 2020.
[18] F. LastnameInam and I. Ur Rehman, "Cybersecurity education training techniques: A systematic literature review," 2023.
[19] W. Shao, "The Development and Opportunity of Educational Mode in the Metaverse Age," vol. 10, 2023.
[20] O. Hajjami and P. Sunyoung , "Using the metaverse in training: lessons from real cases," 2023.

[21] S. . K. Jagatheesaperumal, K. Ahmad, A. Al-Fuqaha and J. Qadir, "Advancing Education Through Extended Reality and Internet of Everything Enabled Metaverses: Applications, Challenges, and Open Issues," 2022.
[22] A. . K. Upadhyay and K. Khandelwal, "Metaverse: the future of immersive training," 2022.
[23] J. . H. Seo, M. Bruner, A. Payne, N. Gober, R. Mcmullen and D. K. Chakravorty, "Using Virtual Reality to Enforce Principles of Cybersecurity," 2019.
[24] P. Wagner and D. Alharthi, "Leveraging VR/AR/MR/XR T aging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations," vol. 2024, 2023.
[25] A. Pantazidis, A. Gazis, J. K. Soldatos, M. Touloupou, E. Kapassa and S. Karagiorgou, "Trusted Virtual Reality Environment for Training Security Officers," 2023.
[26] B. Odeleye, G. Loukas, R. Heartfield, G. Sakellari, E. Panaousis and F. Spyridonis, "Virtually Secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments," 2022.
[27] I. U. Rehman, "Immersive Learning for Cybersecurity: A Virtual Reality-Based Approach for Empowering Users Against Cyber Threats," 2023.
[28] A. R. Dattel, T. Goodwin and H. Brodeen, "Using Virtual Reality for Training to Identify Cyber Threats in the Bridge of a Ship," 2022.
[29] L. Klooster, R. Delden and J.-W. H. Bullée, "First Steps to Improve Cybersecurity Behaviour: A Virtual Reality," 2023.
[30] J. Hamari, Z. Legaki and N. Xi, "Gamification," Hawaii, 2023.
[31] S. Scholefield and L. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," 2019.
[32] T. van Steen and J. R. A. Deeleman, "Successful Gamification of Cybersecurity Training," vol. 24, no. 9, 2021.
[33] M. Armstrong and R. Landers, "Gamification of employee training and development," vol. 22, no. 2, pp. 162-169, 2018.
[34] Majuri, J. Koivisto and J. Hamari, "Gamification of education and learning: A review of empirical literature," 2018.
[35] L. Homner and M. Sailer, "The Gamification of Learning: a Meta-analysis," vol. 32, 2019.
[36] J. Vermeir, M. White, D. Johnson and G. Crombez, "The Effects of Gamification on Computerized Cognitive Training: Systematic Review and Meta-Analysis," vol. 8, 2020.
[37] Crouch, C.H and E. Mazur, "Peer Instruction: Ten years of experience and results," vol. 69, no. 9, p. 970–977, 2001.
[38] Z. z, G. Zhang, S. Jin, J. Wang, Ma and N. , "Investigating the effect of peer instruction on learners with different cognitive styles in VR-based learning environment," p. 11875–11899, 2022.
[39] A. Zaher, M. Faridee and V. Janeja, "Measuring Peer Mentoring Effectiveness in Computing Courses: A Case Study in Data Analytics for Cybersecurity," Hyderabad, India, 2019.
[40] W.Johnson, "Development of Peer Instruction Material for a Cybersecurity Curriculum," 2017.
[41] B. Scheider and P. Asprion,, "Peer Instruction as Teaching Method in Cybersecurity and Data Privacy," vol. 12, 2023.
[42] G. Pernul and L. Englbrecht, "A serious game-based peer-instruction digital forensics workshop," 2020.
[43] V. Roussev and I. Ahmed, "Peer Instruction Teaching Methodology for Cybersecurity Education," vol. 16, no. 4, p. 88–91, 2018.
[44] P. Jansen and F. Fischbach, "The Social Engineer: An Immersive Virtual Reality Educational Game for Raising Awareness about Social Engineering Attacks," 2020.