An XR-Driven Digital Twin Platform for Cybersecurity Education

Anthony Lee

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Engineering

Thomas L. Martin, Chair
Denis Gračanin
Jeffrey Scot Ransbottom

December 11th, 2024
Blacksburg, Virginia

Keywords: Artificial Intelligence, Digital Twins, Education, Extended Reality, Internet of Things, Virtual Reality

An XR-Driven Digital Twin Platform for Cybersecurity Education

Anthony Lee

(ABSTRACT)

This thesis investigates the application of digital twins as an educational tool within the domain of cybersecurity, specifically targeting the infrastructure of water treatment plants. A digital twin is a precise virtual model of a physical asset, process, or system, capturing its state, behavior, and interactions in real-time. By integrating live sensor data, historical records, and predictive models, digital twins replicate their physical counterparts with high fidelity, enabling detailed simulations, monitoring, diagnostics, and analytics. This technology supports improved decision-making, predictive maintenance, and operational efficiency across industries by allowing safe testing and evaluation of modifications without altering physical assets. A case study is presented to demonstrate an immersive experiential learning platform that leverages digital twins to provide cybersecurity education. The platform aims to enhance user engagement and reinforce learning by offering hands-on experiences in a controlled virtual environment. In addition, we provide a cost-efficient hardware solution that represents the physical side of the digital twin as connecting it to the actual water treatment plant hardware is unfeasible. The study compares AI-guided learning, facilitated by a Conversational AI agent utilizing Large Language Models, against a non-AI-guided approach. This comparison evaluates the effectiveness of AI in guiding users naturally through the learning process, thereby examining the potential of digital twins to support efficient, cost-effective education across diverse sectors. The results show that presence is significantly increased with the help of an AI character while other qualities and factors remain unaffected. However, we see learning improvement overall and received positive feedback

regarding the system. Users liked the digital twin concept and felt like it really helped them understand the concept thoroughly.

An XR-Driven Digital Twin Platform for Cybersecurity Education

Anthony Lee

(GENERAL AUDIENCE ABSTRACT)

This project explores using virtual replicas of physical systems to create an interactive, hands-on learning platform for cybersecurity education. A digital twin mirrors the current state and behavior of a real physical system, such as a water treatment plant, by incorporating live data, historical records, and predictive models. These models allow for various applications such as product testing and education without risking harm to the actual system. This thesis introduces a digital twin-based educational tool designed to teach cybersecurity concepts in a realistic setting, where users can learn through a realistic experience. To enhance the learning process, we compare two approaches: one where users are guided by an AI assistant and another without AI support. The AI assistant is powered by an LLM in a natural form that helps users walk through learning scenarios and understand complex topics. This research demonstrates how digital twins, combined with AI, can make cybersecurity education more engaging, effective, and accessible across various fields. The goal of the presented work is to help motivate the shift from traditional learning approaches to a more engaging and experiential model, where learners can interact with realistic simulations, actively participate in problem-solving, and apply theoretical concepts in practical, immersive environments that enhance understanding and retention.

Dedication

I extend my heartfelt gratitude to my advisor, Dr. Denis Gračanin, for his unwavering support, mentorship, and expertise in Human-Computer Interaction, which have been invaluable throughout my graduate studies. I am also deeply thankful to Dr. Mohammed Azab for his insightful guidance on cybersecurity concepts. Both Dr. Gračanin and Dr. Azab generously shared their expertise in academic writing, provided the financial support to publish this work, and offered invaluable tips that greatly improved my work.

Acknowledgments

This thesis has received support from the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. An additional thanks to Virginia Military Institute for their collaboration in this Workforce Development Project. In addition, The Virginia Tech National Security Institute's DOD Senior Military Colleges Cyber Institute provided critical sponsorship to this work, particularly as a resource for student development and learning.

Contents

List of Figures

List of Tables

List of Abbreviations

AI Artificial Intelligence

DT Digital Twins

IoT Internet of Things

LA Learning Analytics

LLM Large Language Models

XR Extended Reality

Artificial Intelligence (AI) is the field of study in engineering where intelligent computer systems do the thinking and processing that a human brain would do.

Digital Twins (DT) are a highly accurate virtual representation of a physical asset/system.

Internet of Things (IoT) is used to describe a set of physical objects (Things) that are connected to each other through an internet network. These objects have software and various sensors that are used to collect relevant data that is then shared with various other devices over that network connection.

Learning Analytics (LA) is defined as the area of research where measurements and collection of data is used to analyze learning effects and how to optimize them.

Large Language Models (LLMs) are a type of AI algorithm that uses deep learning and large data sets to generate dynamic content based on user feedback.

Extended Reality (XR) is the general term used for Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR).

Chapter 1

Introduction

1.1 Background

Building physical prototypes to test one's idea can be very expensive in time and money. In addition, sometimes it is not viable to build a physical prototype due to costs and other constraining factors. For example, when constructing a new building in a city, it would not make sense to waste money to build a physical prototype just to then either scrap the idea or make significant changes. However, without a physical prototype, there is no way to see how the construction of new building would affect the city. In other words, we would not know the effects without building it first and analyzing the results after its existence. At that point, too much money would have been invested to make major changes. What if we could solve all of these problems and build prototypes that are both highly accurate and low cost? That is where digital twins can come into play. The term Digital Twins (DT) is a virtual representation of a physical object or process. These digital representations are highly accurate as they are created from real-time data collected from their physical counterparts using IoT devices.

But that is not the extent of what DT can do. Many researchers already worked on expanding the use case for DT. Capabilities can be further enhanced by integrating DT with AI and XR. This combination enables the development of highly accurate, automated, and immersive simulations for a wide range of applications, providing a powerful tool for effective education,

testing, and planning.

As the world relies on more technology for day-to-day tasks, cyberattacks are becoming more prevalent and have more impact on the population. In the context of critical infrastructures, which are essential systems and assets that support societal functions, disruptions to these systems can significantly impact public safety, national security, and economic stability. Hence, enhancing cybersecurity measures in these critical infrastructures is necessary, and the first step to achieving this is through proper cybersecurity education. Cybersecurity refers to the protection of digital assets such as computer servers and networks. An effective education platform in this field introduces students to various cyberattack methods, teach them how to recognize different types of attacks and cover preventive measures, highlighting the importance of cybersecurity. This thesis is centered on the challenge of offering a hands-on learning experience for cybersecurity within critical infrastructures. More specifically, we focus on how DT can be used for cybersecurity education. In this thesis, we describe the development of a physical testbed with IoT infrastructure that cost-effectively replicates the functions of a critical infrastructure. We create the digital twin's virtual component using extended reality (XR), specifically virtual reality (VR), to provide immersive visual effects beyond real-world capabilities. Additionally, we incorporate AI to enable guided learning through natural and conversational interactions and compare its effectiveness to when we don't incorporate the use of AI.

1.2 Motivation

It is impractical to perform real-life simulations or even to build physical prototypes before implementing the final solution in many situations. Sometimes, it is not practical at all to conduct simulations on the physical process due to ethics and safety considerations. Suppose

that we want to provide cybersecurity education for water treatment workers. It would not be ethical to perform any type of cybersecurity training on the actual system. That would impede the water treatment process, which then can have serious consequences such as environmental pollution and adverse health effects to the community that uses that water supply. You may ask what about building another plant just for educational purposes? Yes, we could do that, but that would be very expensive. Alternatively, a virtual replica of the plant can be developed within a digital environment, providing a cost-effective solution that enables a range of simulations without real-world risks while preserving realism. A prime example of the advantages of integrating DT, AI, and XR is the development of engaging, interactive simulations for educational modules.

Cyberattacks are becoming a growing issue and have had devastating consequences for many people. 145 million people's personal information such as Social Security numbers was leaked through Equifax because the company neglected to install the necessary security updates in a timely manner [6, 27]. In May 2021 a cyberattack occurred on the Colonial Pipeline, which is responsible for transporting fuel across the eastern part of the United States. The cause of the attack was through an employee's exposed password that employees failed to protect [14]. This vulnerability enabled a cyberattack on the company's accounting system, disrupting their ability to track payments and process billing from their customers. As a result, they were compelled to shut down the pipeline. The result of the cyberattack was a gas shortage, mass panic, and a significant increase in gas prices. Coincidentally enough as the case study we introduce focuses on water treatment plants, a water treatment plant in Texas was hacked by Russia-linked groups, which caused the water treatment plant to overflow [29]. As demonstrated, humans are the most vulnerable component when it comes to cybersecurity attacks. Even with the most high-tech security system in place, it is useless without properly educated employees who adhere to effective cybersecurity policies [2]. This

is what motivated me to create a new learning platform that aims to fix that.

Traditional educational methods have proven to be ineffective and inefficient due to the repetition of the teaching structure and the lack of interaction. By involving an interactive component, we can allow for greater concentration and enhanced learning [16, 27]. The simulation quality of DT can be significantly enhanced through the integration of XR, which offers a fully immersive and interactive experience. As a relatively new and innovative concept, XR is progressively being adopted across various applications. When combined with DT, XR enables users to interact with multiple objects and navigate the digital twin as if they were physically present while also interacting with the physical system. This immersive interaction facilitates more precise and informed decision-making while also acting as a user interface for the physical system.

A key benefit of DT is that they not only provide a visual model of a product but also enable precise simulations and data collection, supporting more informed decision-making. Integrating AI enhances user accessibility and quality by simplifying complex simulations. For instance, simulating specific scenarios often involves numerous variables, which can be challenging for non-experts. AI, especially LLMs, can reduce this complexity by generating specific conditions from high-level input, effectively translating broad concepts into detailed technical setups. Additionally, AI can process real-time data within the DT, ensuring the simulation reflects current conditions and can predict potential failures or areas of concern. AI can also serve as a personalized guide, allowing users to interact with it as if a tutor were available to explain concepts and answer questions, making education more cost-effective and efficient than traditional methods.

In summary, combining DT, XR, and AI provide an entirely new level of capabilities like never before. Having XR allows for a more immersive experience with the DT which can further expand understanding and engagement. AI offers enhanced comprehension and data

processing abilities, as well as the ability to automate and handle data more efficiently, leading to faster and more precise decision-making. This inspired me to suggest an innovative learning approach in my thesis, which offers an engaging and participatory experience to improve the learning process going forward.

1.3 Key Issues and Research Questions

As discussed in the motivation section, humans are often the most vulnerable and critical element in cybersecurity. The lack of cybersecurity awareness highlights the urgent need for education to address this issue. However, traditional learning methods are often disengaging and may fail to foster a deep understanding of the subject. There is limited research exploring the combination of these concepts to create engaging educational experiences. Additionally, integrating AI language models (LLMs) with XR presents a unique challenge, as these models are typically designed for text-based interactions, which are not ideal for VR applications where a keyboard is not readily accessible. To enhance usability and improve the sense of presence, the AI LLM needs to be presented in a more interactive and engaging format.

Given these problems, the primary objectives of this research include exploring the potential of experiential learning through the developed system, assessing the effectiveness of human-like interactions with AI-driven NPCs in educational settings, and creating a cost-efficient physical testbed with a VR interface that integrates DT, XR, and AI. Ultimately, the goal is to provide an immersive cybersecurity educational platform that enhances the learning experience by combining practical, hands-on activities with cutting-edge technologies. With these objectives in mind, we present the following research questions:

1.3.1 RQ1: How does utilizing an XR-based DT platform for cybersecurity education influence participants' engagement, knowledge acquisition, and ability to interpret system behavior?

It has been demonstrated that the use of XR is increasing rapidly due to its capabilities in providing an engaging and immersive learning experience [16, 19, 40, 42]. However, very few curricula involve the use of hardware and VR in combination. Participants in the user study were asked about their experiences using the developed VR platform and were assessed on the cybersecurity concepts they learned. Metrics evaluated included their knowledge of cyberattacks, system usability, presence, and workload. These responses were collected through various surveys and through an open-ended exit interview format.

1.3.2 RQ2: Does AI-guided learning have an impact on knowledge acquisition and experience when compared to non-AI guided learning?

Ensuring that the developed educational platform is effective and beneficial for learners is essential. Many students are starting to use AI language models (LLMs) like ChatGPT-4o for educational purposes, and while these tools can be highly valuable, LLMs remain relatively immature as they have hallucination effects that cause them to provide inaccurate outputs and other errors [36, 54]. Our goal is to present AI LLMs in a human interactable format, allowing users to engage with them as if they were interacting with another person. However, concerns here arise from the reliability of AI and its potential impact on AI-guided learning.

To answer this research question, we perform a between subject user design where participants are randomly selected to complete the AI guided or non AI guided learning modalities. Users are asked to fill out surveys before and after the study to collect data on user experience metrics and learning outcomes.

More details relating to these research questions and their challenges can be found in Chapter 3.

1.4 Approach

This thesis aims to develop an experiential learning platform that integrates the three concepts: DT, XR, and AI, within the context of cybersecurity education. The motivation for this research arises from the alarming rise in cyberattacks, as detailed in Section 1.2, highlighting the necessity to transition from traditional educational approaches to a more engaging and immersive learning experience.

The proposed approach is based on Kolb's Learning Cycle as it helps connect theory with practical applications to further user understanding. The VR environment consists of two phases: the tutorial phase and practice phase. The tutorial phase fulfills the first half of Kolb's learning cycle while the practice phase fulfills the second half of Kolb's learning cycle (Figure 4.1).

To establish a foundational understanding, we begin with a literature review (Chapter 2), which dives into existing research related to XR, AI, and DT. This review explains how these concepts have been previously employed and identifies critical research gaps that this thesis seeks to address.

As part of a Workforce Development program in collaboration with Virginia Tech and Vir-

ginia Military Institute, we create an Experiential Learning Platform in the context of cybersecurity education for water treatment plants It leverages a VR user interface for the DT concept. The platform has two distinct phases: a tutorial phase to familiarize users with the system and teach them about the cyberattacks and a practice phase for hands-on application of the knowledge they just learned. We conduct a between-subject user study to compare two different modalities presented in the practice phase: AI-guided and non-AI-guided approaches, with further details provided in Section 4.4.4.

On the physical front, we construct a cost-effective hardware testbed that replicates the essential functionalities of a water treatment plant using IoT devices. This infrastructure facilitates cyberattack demonstrations, allowing participants to observe and interact with cyberattack scenarios in real-time. Detailed implementation aspects of this testbed can be found in Section 4.4.3. Throughout the educational experience, users witness the ramifications of cyberattacks by executing them on IoT devices, with the implementation details elaborated in Section 4.4.2.

The user study participants are randomly selected to participate in AI guided learning or non-AI guided learning. This helps us assess the effect of using AI NPC characters. Users are assessed on their cybersecurity knowledge before and after the study to obtain data on their learning improvement. In addition, we evaluate user satisfaction with the participants' experience with the system by obtaining various metrics described in Chapter 6.

The system's implementation and the user study results are subsequently linked to our research goals and questions in Chapter7. This provides further insight into how the work here achieves them and how key features play a contributing factor.

1.5 Contributions

This thesis aims to introduce a new type of learning mechanism where user experience is the contributing factor to learning and concept retention. More specifically, a case study is provided that demonstrates how we can develop a system that combines the three concepts (XR, AI, DT) to potentially improve cybersecurity education in the context of water treatment plants. The system's capabilities are demonstrated through a user study to evaluate its impact on learning, its influence on human behavior, and its overall effectiveness. A discussion is then provided that analyzes our findings and how these findings provide suggestions for future work.

Furthermore, this work has resulted in several scholarly contributions, culminating in three academic publications. These include papers presented at the HCI International 2024 [27] and IEEE UEMCON 2024 [37] conferences, as well as a journal paperr [13].

The HCI International paper highlighted the significance and motivation driving the project, as well as the proposed overall architecture of the platform. It provides a comprehensive explanation of the design and functionality of each component, detailing how they interact and integrate seamlessly.

Building on this foundation, my subsequent paper, published and presented at IEEE UEMCON, focuses on the development and design of the VR component. This work introduces Kolb's learning cycle as the theoretical foundation of the VR system architecture and includes a user study evaluating the component's effectiveness and feasibility.

Expanding further, the journal paper explores a novel framework that integrates XR and Generative AI within a gamified platform. This paper examines user behavior within the system and utilizes my thesis work as a case study to validate the framework, demonstrating its potential in practical applications.

1.6 Thesis Structure

Chapter 1 provide an overview of the relevant concepts and demonstrates the need and motivation for this research. It also covers the proposed research questions and a high level overview on the proposed approach.

Chapter 2 presents a review of existing research on DT, XR, and AI and its application within critical infrastructures and learning. It examines their use in product design, existing digital twin frameworks, and educational applications to support the case for the relevance and potential benefits of this thesis. The literature review dives into the current research gaps and how filling in those research gaps can be beneficial.

The problem definition is presented in Chapter 3, where we discuss the issues we aim to address in the research, along with the justification for how the research questions align with these challenges.

The thesis then dives into the specific case study in Chapter 4 where we detail the development of the proposed learning platform and the various features it provides. Details regarding the study design are provided in Chapter 5 where we discuss the format and details of the user study.

This is followed by an evaluation of this experiential learning platform in Chapter 6 which provides researchers with insight into how to adopt these ideas to improve the future capabilities of these concepts. Evaluation of this case study analyzes how effective this type of learning tool is for people who are new to the concept of cybersecurity when compared to traditional learning methods.

The results provided from Chapter 6 are then analyzed and discussed further in Chapter 7 where we talk about some theories as to why we obtained those particular results. We also

provide some observations and discuss areas for improvement in future work. Chapter 8 summarizes the work presented in this thesis.

Chapter 2

Review of Literature

Numerous studies have initiated research into the individual use of DT, XR, and AI, as well as the integration of these technologies in pairs for diverse applications. However, there is a lack of focus on exploring the potential of merging all three components. Research lacking the XR component lack the immersive experience that could be provided to a user to help simulate real-life scenarios on an entirely different level. This, in turn, aids stakeholders in making more informed and educated decisions thanks to interactive experiences. Incorporating AI provides seamless automation for processing large amounts of data being received from various sources and reflecting that data onto the DT environment. It can even be used to generate dynamic content which is especially helpful in education scenarios. In addition, it can assist in analyzing intricate data, facilitating the translation of technical information into a more accessible format for beginners, and ultimately aiding students in comprehending complex concepts. Predictive algorithms can be formulated that help provide further analysis capabilities that humans are unable to perform. This literature review dives into the various research applications for the fields so far and analyze how they could be further improved.

2.1 History of DT

This section aims to introduce some historical context of how the realm of DT came to light. Originally it was not called a *DT*. It was only called a *twin* back in the 1960s. The term *twin* was formulated by the National Aeronautics and Space Administration (NASA). NASA employed this concept to create replicas of their space vehicles to evaluate their effectiveness. This concept also helped NASA troubleshoot various issues that came to light when astronauts were in space. A notable example is the Apollo 13 space mission, where the concept of a twin evolved into a DT during the rescue operation. An oxygen tank explosion caused damage to the main engine of the spacecraft. The astronauts were stranded but thanks to the team on the ground, engineers were able to create a DT model of the Apollo 13 spacecraft that allowed them to provide the astronauts with a solution to come home safely. Given that the rescue mission was a success, it further proved the usefulness of the DT concept [1, 33]. NASA continues to use the DT concept to ensure the safety of their vehicles and to prevent anything like Apollo 13 from happening again.

However, NASA is not the organization that gets the credit for developing the DT concept. The person most known for getting the DT concept recognized is Dr. Michael Grieves, a Research Scientist/Executive Director at the DT Institute. He first introduced the DT concept in 2003 as a part of his course on Product Lifecycle Management at the University of Michigan [18]. This was during a time when the digital world was extremely new and not commonly used. On top of that, most of the manufacturing data was collected manually and physically on paper, hence the lack of automation and digitalization.

The next notable progression of DT took place in 2012 when NASA applied the DT concept to collect data from their vehicles remotely. Their vehicles were integrated with various computer systems that allowed them to gather data on their vehicles' health to formulate a

dataset to perform high-fidelity simulations [20]. This overall contributed to the significant improvement of the safety and reliability of their spacecraft [17].

Research into the DT field continues to expand as more and more industries begin integrating IoT devices for many different applications. Especially into Cyber-Physical Systems as a part of the Fourth Industrial Revolution Initiative founded by Germany. The Fourth Industrial Revolution was created in 2011 by the German government to make Cyber-Physical Systems more intelligent. They aim to do this by using real-time data and modern communication technologies to create a more intelligent and autonomous manufacturing process. Many other countries have also followed suit and are forming collaboration projects to support this initiative [50]. To provide context on the first three industrial revolutions here is a list containing their definitions:

First Industrial Revolution - The transition of manual labor for product production to the use of machines powered by steam and water.

Second Industrial Revolution - The introduction of electricity into factories. Helped create modern production lines that resulted in a more efficient manufacturing process.

Third Industrial Revolution - Introduced computer systems such as Programmable Logic Controllers (PLC) and communication technologies into the manufacturing process that created automation in production mechanisms.

2.2 Product Design and Prototyping Applications

Presently, many product designs overlook digital design aspects and predominantly rely on traditional approaches, crafting and evaluating physical prototypes despite the industry's shift towards digital methodologies. This divergence largely arises from a lack of data-driven

practices in both virtual and physical design realms. Furthermore, when both virtual and physical components exist, they often lack integration, undermining their combined utility. On top of that, there is the exponential growth in data volume requiring collection and analysis. Thus, there is a pressing need for streamlined methods to gather and analyze this expanding dataset efficiently [18]. The approach needs to change as it is less efficient and generates more costs during the production process. Industry 4.0 also known as the fourth industrial revolution [25] aims to achieve this goal by converting the manufacturing process to be more intelligent to provide for a more efficient, dynamic, and less time-consuming process.

Industry 4.0 is heavily reliant on the concept of Smart Manufacturing, which is the use of real-time data to make the appropriate changes needed during the manufacturing process. This process is used to keep quality control in check and possibly identify various flaws. The main issue is that having everything done manually leads to extra costs, due to manpower and time. Hence the introduction of AI into the manufacturing process can help alleviate these factors. Aphirakmethawong [4] emphasizes the importance of smart product design to be successful in the industry. The author proposes AI as the solution for smart product design as it can analyze various data points such as customer needs and ergonomics much quicker to facilitate development.

Fei Tao [43] proposed a DT-based product design process that aims to solve various issues of the traditional physical design process. One such issue is the inability to monitor physical systems with high fidelity remotely. Adding a virtual model adds the convenience of being able to monitor systems remotely. This design approach also further supports the issue of data collection. Tao emphasizes the issue of having to analyze data from various sources which leads to an unorganized data collection methodology. His solution aims to fix that as DT can gather real-time data from the physical system and consolidate it with other data all

under one roof. His work also supports a new design approach of receiving customer feedback as they are developing the product. It would be infeasible to replicate the physical system for each customer or have the customer travel to where the physical product is located. With DT, there is now a virtual component that can be shared with customers remotely.

This research is a great step in the direction of Industry 4.0 but this work still heavily relies on the use of physical prototypes which increases costs and the amount of work. By incorporating XR, the DT model can be brought to life. Interaction capabilities allow users to determine ease of use, defects, and various other problems before formulating a physical prototype. Hence significantly reducing costs and manufacturing time. It also provides an easier solution for testing purposes as testing in an XR environment, also allows for simulation parameters to be changed quickly, and is less costly since no physical equipment is needed to form the desired testing environment. AI not only assists with the data collection here but can also be used to help create various parameters and scenarios delivered simultaneously while also performing real-time data analysis. Examples of potential analysis capabilities include predictive algorithms for product defects and unsuitability in various scenarios. Some possible use cases for AI are described in Section 2.2.1.

2.2.1 Current DT and Conceptual Frameworks

Catalano proposed a DT framework where XR is used to improve business performances such as in a production factory. The framework involves two types of operators: on-site and off-site. The on-site operator is in the actual manufacturing plant and wears an XR device such as the Microsoft Hololens. The XR device allows the operator to use various apps that provide a set of interactive smart functionalities and help operators perform their jobs with utmost accuracy. The off-site operator can access the framework using a web app

that provides them with real-time data from machines and a simulation tool [8]. A critical element absent from the proposed framework is the incorporation of AI for processing real-time data. The paper's referenced software, AnyLogic [9], does not inherently employ AI for data processing and simulation generation. Instead, it requires manual configuration by users to meet their specific simulation and application requirements. Grieves [18] also proposes a similar framework in the realm of manufacturing to emphasize the importance of a data link between physical and virtual processes. He proposes a Unified repository be used to link the two together. The Unified repository would contain data populated from both the physical and virtual assets where they can be classified and further used as needed.

Having a person analyze all of the data manually can be severely overwhelming and lead to costly mistakes. Integrating AI into both Grieve's and Catalano's work could significantly enhance this process by providing seamless automation and speedier configurations. Within Catalona's framework, an on-site operator could leverage AI for real-time feedback on their actions. Instead of manually adjusting each parameter and observing outcomes, users could direct the AI to simulate specific scenarios, with the AI autonomously formulating the necessary intricate details. Moreover, the AI could continuously assess the operator's decisions, offering dynamic feedback on selected actions. AI could proficiently sort and analyze real-time data for off-site operators, preemptively spotting failures or imperfections that might evade human detection. Additionally, AI integration could streamline the simulation process, enhancing predictive capabilities and significantly simplifying user interaction within the simulation environment.

2.3 DT Applications in Critical Infrastructures

There are many benefits to applying a DT concept to critical infrastructure applications. One of which is the ability to collect real-time data from the cyber-physical system of the critical infrastructure. By providing this data collection, AI can enhance analysis capabilities to prevent future failures and improve cyber breach detection. More specifically, AI can be utilized as part of an Intrusion Detection System for monitoring anomaly detection or it can be used to provide dynamic feedback or suggestions for preventative maintenance and improving water quality. Snijders et al. [41] uses *Temporal Convolutional Neural Networks* in combination with DT to create a predictive algorithm meant for testing certain conditions in *Cyber-Physical Energy Systems*. Xu et al. [49] demonstrates that AI and DT can be used to perform anomaly detection. Anomaly detection is the detection of abnormal behavior in a given system which can be used to detect a potential breach in security. The benefit of having a DT compared to just simply using an AI model for anomaly detection is the ability for continued learning. More specifically, it can handle what is called *unlabeled data*, which is data that has not been classified or within the scope of the AI's knowledge set, to learn and adapt while the cyber-physical system continues to operate. The experiment resulted in an anomaly detector that outperformed the majority of other notable anomaly detection systems demonstrating its effectiveness. In addition, the study tested with and without the use of a DT to collect real-time data and further showed the need for a DT to achieve better performance.

Wei et al. [45] advanced this research by proposing a DT framework that integrates the contributions of Snijders et al. [41] and Xu et al. [49], with a specific focus on enhancing AI capabilities within cyber-physical systems, particularly within water treatment facilities. Notably, their work emphasizes the significance of continuous predictive modeling by AI,

leveraging real-time data for both forecasting and model refinement. Empirical findings demonstrate the indispensable nature of this framework, demonstrating a marked reduction in classification errors compared to approaches not incorporating real-time data.

Similarly, Zhao et al. [52] contributes to this domain by developing a DT for water treatment plants, addressing challenges that are present in traditional manual labor practices. Through this work, they aim to dynamically represent plant operations digitally to allow operators to discern issues imperceptible through direct observation. Additionally, the framework facilitates automation functionalities, such as temperature regulation. Zhao employs advanced machine learning models including Long Short Term Memory and Gate Recurrent Units to forecast water quality based on specific plant data inputs.

This type of work is not just specific to water treatment plants and can be applied to many different applications. White [46] discusses the use of DT for the modeling of a smart city to take advantage of the large presence of building information models (BIM). He focuses on taking advantage of this to provide an accurate 3D model of a smart city where various simulations can be conducted. Examples of simulations include new city construction projects, traffic pattern analysis, and severe weather conditions. This model can then be provided publicly online where residents of the city can provide feedback on the proposed changes or be well-informed about potential city conditions to provide more transparency. Although the introduction and related work sections of White's paper talk about AI and ML, it is unclear if his solution uses any form of AI for data collection and processing.

2.4 Current Experiential Learning Experiences

Traditional teaching methods are becoming inadequate for students as it is hard to remain focused and does not expose the new concepts clearly or engagingly [16]. Many researchers

have begun to explore how to provide a new type of learning experience that can further improve material retention through realistic experiences. This is known as Experiential Learning. Gironacci proposed integrating Natural Language Processing with AI and XR to create a system that delivers dynamic feedback based on user input and interactions within the training simulator [16]. An XR simulator [51] for learning how to play the guitar aims to improve traditional learning methods by providing real-time feedback and guidance. It aims to teach students how much force to apply to guitar strings and how to time the strokes correctly. The simulator does not incorporate AI which could be used to further enhance the learning experience. AI could analyze the user's behavior to generate dynamic feedback unique to the players' actions and also help in generating dynamic lesson materials. The paper noted that it wanted to provide guidance markers that help users understand their finger placement on the guitar while playing a song. But this is unique to the specific song they are playing so to reduce the burden of programming all of that manually, we can train the AI to do it for us. We do achieve something similar in the case study (Chapter 4) by having an AI agent guide users throughout the education process and provide feedback based on user responses.

Experiential learning is even being considered for various sports such as soccer. An XR environment is being created to train soccer players in executing goal kicks, utilizing image recognition software and a camera system. [34]. The camera is used to measure various parameters such as ball speed and axis rotation to help create a trajectory for the player. AI can be incorporated into this use case to analyze the parameters and autonomously provide personalized suggestions for improving the kick. In other words, AI can be used as a virtual coaching assistant.

Komninos [24] proposes a DT system to solve the challenges of Environmental Education within Urban areas for young children. He achieves this through a smart birdhouse that

collects various data such as sound and images which can then be portrayed through the birdhouse DT that allows children to experience the birds in the natural environment from any location. The problem with this solution is that a Raspberry Pi device with a tiny screen is used as the DT. This hardly produces an enjoyable experience let alone a realistic one. Further work can be implemented to incorporate Komnino's solution with an XR component to provide further realism.

2.5 Learning Analytics (LA)

The term Learning Analytics is defined as the area of research where measurements and collections of data are used to analyze learning effects and how to optimize them. Currently, this area of research is premature and it is agreed upon that there are no effective learning behavior indicators or ways of extracting these behaviors from virtual environments [48]. It has been demonstrated that LA and learning design has strong correlations with each other [30, 35, 47].

Xiao et al. [48] applies LA in the context of Mobile Learning Support Systems that integrate with AR. He gathered various data from participants that analyzed the subject's interaction with the training material such as reading speed and then made correlations to the normal learning speed to demonstrate their platform's effectiveness and usability. On top of that, the LA model also allowed for the analysis of user behavior to determine if a participant treated the learning seriously to reduce bias in the data. Similarly, Sharma et al. [39] used eye-tracking data to form a Gaze-based Learning Analytics Model to track the students' attention with online digital content. The model displayed students' attention levels and guided their focus on the screen, leading to enhanced learning outcomes.

2.6 Methods

2.6.1 Research Topics

Conducting this literature review allowed for an understanding of the current applications of XR, AI, and DT and its potential for further innovation within various applications. This review provided an analysis of the research gaps in current studies and how these gaps could be filled. The following learning questions were used during the literature analysis.

LQ1: What are the current applications and interaction techniques for DT, XR, and AI? Especially in the critical infrastructure sector.

LQ2: How can DT be combined with AI or XR for practical application use?

LQ3: How has the use of DT and XR made an impact on various industries?

LQ4: How are XR, AI, and DT currently used in the education sector?

LQ5: What are some ways to measure and evaluate learning?

2.6.2 Inclusion Search Criteria and Methodology

To ensure that only relevant and quality papers were used for the Literature Review, we only used Virginia Tech library resources and tools. The library provided access to many academic paper databases but the following databases were primarily used: IEEE Xplore, SpringerLink, ACM Digital Library, MDPI, and Science Direct. On top of that, the following criteria were used in identifying papers.

1. Was a published academic paper

2. Paper was found through notable conferences such as HCI International and IEEE-sponsored conferences.
3. Had a focus on at least one of the following concepts: DT, XR, and AI.
4. Focused on Academic Research

The search methodology consisted of the following steps:

1. Use a combination of the keywords mentioned in 2.6.3 to find relevant publications on the databases mentioned above.
2. Determine if the publication was of interest and relevance by reading the abstract, introduction, and conclusion sections.
3. Within the papers of interest, look at other relevant sources that were cited to see if they were also of relevance by repeating step 2.

2.6.3 Keywords Used

The following keywords were used both separately and in combination when searching for relevant papers:

1. Artificial Intelligence
2. Digital Twins
3. Virtual Reality
4. Augmented Reality
5. Mixed Reality

6. Extended Reality

7. Education

8. Learning Analytics

2.7 Discussion

The goal of this literature review is to dive deeper into the current research that has been done in XR, AI, and DT and analyze potential research gaps to provide a better context for the goal of my research. Which is to demonstrate how AI, XR, and DT can benefit from being used together. The literature contains five sections to achieve this goal. We start by diving into the history of DT and how it was introduced into the world. We saw that DT has practical uses for many different applications and can be used as a life-saving tool, further demonstrating the essential role of DT in practical applications.

The second section explores the current flaws of the heavily physically reliant design process. We analyze the proposed solution and add some potential benefits of incorporating XR and AI into their existing solution. A great example of the importance of this work can be seen in New York City's subway system. Currently, the Metropolitan Transportation Authority is substantially in debt and projected to go deeper in the coming years [12]. Yet they are wasting millions of dollars on various pilot programs that have proven to be ineffective [11, 44]. $700 million was spent just to test a set of new turnstiles that were then found to have significant flaws. By implementing a digital design process, as mentioned in Section 2.2, a virtual replica could have been created, and a user study could have been conducted to identify these flaws, thereby saving the MTA the $700 million cost of manufacturing these ineffective gates.

Section 2.2.1 continues the topic of product design and analyzes a proposed DT framework for the manufacturing sector. We specifically discuss how AI can be beneficial here to determine design flaws before they occur. As humans, we are unable to process data and make predictions quickly when compared to what AI can do. Hence leading to human errors and significant quality control issues. Honda recently recalled more than 750,00 vehicles due to airbag safety issues [3]. Boeing's 737 Max has recently had many quality control issues due to dozens of issues that have been discovered over the years [7]. The most notable one was the incident with Alaska Airlines where an emergency door panel blew off the plane mid-flight. AI here could have been used to conduct various simulations and predictive algorithms for long-term durability to determine flaws ahead of time.

As the case study focuses on cybersecurity education for critical infrastructures, we thought it would be appropriate to review the current work going into DT applications for critical infrastructures (Section 2.3). The section demonstrates the potential benefits of applying the DT concept for critical infrastructure applications. AI can be used for real-time data collection for various applications such as studying system behavior, cybersecurity protection, and preventative measures. So much data is continuously being generated and it is infeasible for humans to process and keep up thoroughly. AI alleviates this burden on humans and provides capabilities to detect system failures before they even occur. This is an important factor for critical infrastructures as they run 24/7 and can not afford to become inoperable. As humans becomes more heavily reliant on computers and digital systems, the attack surface for cyberattacks continues to increase. Section 1.2 has already demonstrated the capabilities of these types of attacks. By having AI perform anomaly detection, sophisticated firewall systems can be built to detect intrusions that other mechanisms failed to prevent in real-time.

In the case of smart cities [46], AI can be used to simulate the city in real-time by processing IoT data being received to then accurately reflect it on the DT. In addition, it can be used

to simulate various conditions to determine flaws in a proposed design. We can ask the AI to simulate bad weather such as heavy rain to determine if heavy rain will cause flooding in certain areas or ask the AI to simulate how the city would be with an increased population due to a new building being added. Which can then provide hypothetical traffic patterns and effects on public transit. Although there is a 3D model of the DT, further immersion can be provided if XR is incorporated. More specifically, XR can provide the ability to walk through the environment and interact with various objects. For example, if a new subway station with new technologies is proposed, XR will allow stakeholders to walk through the new proposed subway station and interact with the various technologies. This will allow them to visualize and experience the proposed project before building it allowing them to save millions of dollars and allow for easier design refinements.

Experiential Learning is an important concept that should be explored further due to its effectiveness in portraying actual scenarios clearly to the students. The use of some type of video or immersive experience has resulted in better long-term memory retention. VR has been proven to support this immersive experience by providing interactive capabilities that change the way students portray themselves in the learning scenario [22]. Experiential Learning through VR is more effective than traditional learning methods due to its ability to provide details beyond traditional textbooks and PowerPoint presentations. Students can experience first-hand what it is like which provides a better sense of imagery for deeper comprehension. On top of that, the DT concept is rarely used for learning purposes. If added, it can help students further visualize the concepts in practicality on top of VR. My thesis aims to continue this trend. Therefore, this literature review includes a section on how VR has been utilized for experiential learning so far, providing the necessary information to expand upon that research and integrate AI and DT to further enhance experiential learning.

It is challenging to identify the key attributes of human behavior for evaluation, making

it difficult to establish a standard method for measuring human behavior [48]. On top of that, different types of learning methodologies would require different types of analysis methodologies. As DT and VR are not highly used in the education field yet there is no standard way to measure human behavior for learning outcomes. The goal of Section 2.5 was to introduce the ideas so far that have been used to gauge and evaluate different learning platforms. More details about the challenge we are faced with are presented in Section 3.2.5.

Chapter 3

Problem Definition

In the previous chapter, literature review provided an overview of the history of DT and the various applications it was used for. In addition, it covered potential use cases within critical infrastructures and talked about how XR has proved to be beneficial for educational purposes. However, little research looks into how DT, XR, and AI can be combined for further potential, especially in education. It is often difficult to visualize the importance of the DT concept due to its rare use and the lack of education on the topic. However, these concepts are beginning to be implemented in the industry but there is a gap between academic education and industry needs. My thesis is connected to a collaboration within a workforce development program involving cadets at the Virginia Military Institute and graduate students at Virginia Tech. Through this program, we strive to enhance students' readiness for the workforce by exploring the development of these new technologies, while also examining the impacts of applying these concepts within the education sector. To achieve the goal of educating students about the DT concept while creating a platform to study the effects of a proposed system being used for educational purposes, we create an Experiential Learning platform for cybersecurity education in the context of water treatment plants. By developing and testing this platform, we strive to contribute to research for combining DT, XR, and AI concepts and motivate the change from traditional learning methodologies to a more immersive and engaging method.

3.1 Research Questions

Many methods of teaching have been proposed, yet we are still favoring the traditional presentation style of learning that provides no sense of engagement and decreases learning outcomes [22]. Learning experiences using VR provide immersion and visualizations that further enhance the student's ability to comprehend teachings. It has already been shown in various research that VR is effective for educational purposes. My primary objectives of this thesis is to study the learning effects of using VR as a user interface for DT platforms. While also studying what happens when DT are supplemented with additional features such as being able to interact with an LLM that provides the users with dynamic feedback based on user interactions and input. Through this work we are also contributing to workforce development and preparing the next generation of engineers on the concept of DT and VR. We aim to use these concepts to promote enhanced problem-solving and critical thinking. Further research is needed to determine if combining these concepts will provide for a better learning outcome or make learning overcomplicated. My thesis aims to answer the following research questions.

RQ1: How does utilizing an XR-based DT platform for cybersecurity education influence participants' engagement, knowledge acquisition, and ability to interpret system behavior?

RQ2: Does AI-guided learning have an impact on knowledge acquisition and experience when compared to non-AI guided learning?

As discussed in Chapter 1, traditional learning methods are not feasible due to their inability to portray concepts clearly and engagingly. Furthermore in the context of the case study, using the actual water treatment plant for educational purposes to portray effects would

be infeasible due to high equipment costs and various ethical concerns involved. These are some of the challenges that interfere with providing an effective methodology for teaching cybersecurity concepts in the context of water treatment plants. The research we conduct aims to solve the visualization problem by using a VR interface to portray the effects of cyberattacks on the system. Since the infrastructure at the real water treatment plant can not be used, we create a more cost-efficient physical component of the DT that aims to mimic all essential hardware components of the water treatment plants and provide the concept of connectivity between the virtual environment and physical mechanisms through IoT devices.

Generative AI is an emerging concept that people have been using as a tool in many fields, from coding to writing it has helped people succeed in a specific task. In Chapter 2 we have shown the potential of using generative AI to create content based on user feedback and how it has proved to be effective. In addition, it has proven useful in the education realm, more specifically in the field of Computer Science and Engineering Education [26, 53]. We aim to further explore AI's capabilities as a virtual teacher and explore its effectiveness.

3.2 Research Challenges

Various design and development challenges need to be dealt with to truly answer the proposed research questions. The list of challenges below presents key aspects of developing the educational tool.

Using LLMs to generate attack commands and dynamic content for guided learning:

LLMs are far from mature. Consistency and accuracy are required for education platforms to be effective which LLMs tend to lack. Our goal is to leverage LLMs to create an AI-guided experience that enhances user engagement in a natural form. We require

a method to transform text-based LLM models into naturally interactive, person-to-person conversations.

Connecting the Virtual Environment to the Physical Environment:

To ensure the Virtual Environment consistently mirrors the physical systems accurately, a real-time data link is needed. In other words, a reliable and efficient communication protocol must be established to maintain proper and continuous interaction between them.

Cost and Accuracy:

In the context of water treatment plants, it would be unreasonable to replicate the entire plant to perform demonstrations due to the high costs. So a cost-efficient way needs to be determined. On top of that, the physical environment needs to accurately reflect the core elements of the water treatment process to support realism.

Security:

As we will be demonstrating cyberattacks on the educational platform by performing them, ethical considerations need to be considered to ensure the safety of the public and the equipment to prevent damage.

Evaluation:

We need to ensure that the proposed system provides students with the appropriate learning outcomes. To do that, we need to evaluate its effectiveness, and ease of use.

3.2.1 Using LLMs to generate attack commands and dynamic content for guided learning

Although LLMs have proven to be a really helpful tool, they are far from mature and can still produce results that are inaccurate [26, 53]. Hence we can not rely on Generative AI 100% of the time. They tend to generate fantasized information and have trouble following simple instructions consistently. As we need to use AI to generate dynamic content for users in the Virtual Environment and generate attack scripts, these factors are important. If the platform is only able to generate attack scenarios sometimes or provides irrelevant information, this can misguide users or impede them from visualizing the cybersecurity concepts in action.

Educational learning platforms tend to omit the capabilities of AI and have static content for users to work with. This prevents users from asking questions to further their understanding unless an instructor is present which is not always the case. On top of that, programming for all possible user responses is unfeasible and tedious. If we can integrate AI to generate dynamic content, it will allow students to receive dynamic feedback based on their inputs and provide personal engagement that enhances their learning experience. Also interacting with LLM's like ChatGPT has primarily been through text-based chats which is not suitable when providing engagement and immersiveness through a VR application. To enable more natural interaction for students on the platform, a speech-to-text and text-to-speech system must be implemented. Additionally, the representation of the AI in the VR environment should be designed to provide a sense of realism and naturalness.

3.2.2 Connecting the Virtual Environment to the Physical Environment

The purpose of a DT is to have an accurate virtual replica of the physical system. Therefore, a communication mechanism is required between the virtual and physical environments. It is essential to identify a suitable communication protocol that is compatible with both the virtual environment program and the hardware forming the testbed to establish a real-time data link. The communication platform needs to be accommodating of transmitting data in parallel on the same network while making sure the data is routed appropriately.

3.2.3 Cost and Accuracy

To make this educational platform accessible to everyone, we need a cost-effective solution. Building a large-scale replica of a water treatment process is expensive because the commercial equipment used in real plants is pricey. Additionally, maintaining and operating such a replica would not be sustainable in the long run due to utility and maintenance costs.

At the same time, the hardware platform should accurately reflect the core elements of the water treatment process to ensure realism and accuracy. This is important in the context of education as it allows students to make real-world connections when going through the scenarios. In the world of DTs, creating a cost-effective replica of the physical hardware system is crucial. While a fully functional replica might be ideal, the expense often outweighs the benefits especially since one of the goals is to provide a cost-effective education platform that can easily be adapted. This translates to significant cost savings, improved safety, and ultimately, a more efficient and reliable physical system.

3.2.4 Security

As cyberattacks are performed on the developed systems, using the actual water treatment plant infrastructure is unacceptable since it can pollute surrounding ecosystems and the water supply, along with damaging expensive equipment. Additionally, we must ensure that our system adheres to legal regulations, as conducting cyberattacks is both unethical and illegal. Therefore, it is crucial to host our platform on a private network within a closed loop to prevent cyberattacks from accessing unauthorized networks or impacting unrelated clients. Within this closed-loop network, no non-target devices should be connected to avoid the risk of their systems being compromised.

3.2.5 Evaluation

No learning platform is perfect in the beginning, and there is always room for improvement. Evaluating system usability is relatively straightforward, thanks to numerous established Human-Computer Interaction standards. However, measuring human behavior when engaging with the material presents its own set of challenges. This is where Learning Analytics (LA) becomes essential. We need to develop a methodology that can analyze the users retention of cybersecurity concepts and provide insights into user engagement. This enables us to identify strengths and weaknesses within the curriculum, allowing for further design enhancements. Another challenge is the interpretability of results, as educators must decipher complex data to make informed decisions. Misinterpretation poses a risk, potentially leading to inappropriate interventions.

Chapter 4

Approach

4.1 Traditional Learning vs Experiential Learning

In this section, we define the terms traditional learning and experiential learning and then provide a comparison of the two techniques to provide a clear understanding of our approach. Traditional learning, also known as passive learning, involves students receiving information from an instructor and processing the information they have learned. The most common and widely used example of this methodology today is lecture-style learning where students simply attend a presentation and take notes. This method provides no engagement or hands-on experience for students to understand concepts in greater depth hence making it more difficult to process the information.

In contrast, experiential learning, also known as active learning, involves students actively participating in the learning process. Instead of passively taking notes during a lecture given by an instructor, learners actively engage with the material through some form of interaction, allowing them to gain practical experience. The experiences gained through this method result in a deeper understanding of the material and improved retention of learning.

4.2 Kolb's Learning Cycle

The framework that is followed to provide an experiential learning platform is known as Kolb's Experiential Learning Cycle [23, 31]. This model was chosen as it emphasizes learning through experience, making it ideal for applications that require a combination of theoretical understanding and practical implementation, such as cybersecurity, where hands-on activities and real-world scenarios are crucial for understanding and mitigating complex threats. Kolb's main theory was that learning is most effective when users go through the experience and can reflect upon it. The cycle involves four stages (Figure 4.1). The first is concrete experience. During this stage, users are first introduced to the concepts so they have a high-level idea of what to expect. Following the completion of this stage, users then watch the learning being applied in a realistic scenario to provide further understanding. This stage is known as Reflective Observation. Once the users encounter the experience, they can use what they have just seen to process further the concepts they are learning and make any adjustments to their knowledge that they may have believed was correct. This stage is known as Abstract Conceptualization. Once users feel they have a good understanding of the concepts, they can reinforce their understanding through the Active Experimentation stage. This is where learners would apply their knowledge to realistic scenarios and learn by experience.

Inspired by the motivations in Section 1.2, the approach taken was through a case study that was conducted as a part of a Workforce Development collaboration between Virginia Tech and the Virginia Military Institute. The case study aims to study the effects of learning through the core concepts (DT, XR, and AI) in cybersecurity education for water treatment plants. The project seeks to offer an immersive educational experience that enhances plant workers' awareness of cyber threats and the potential consequences of failing to implement proper precautions.

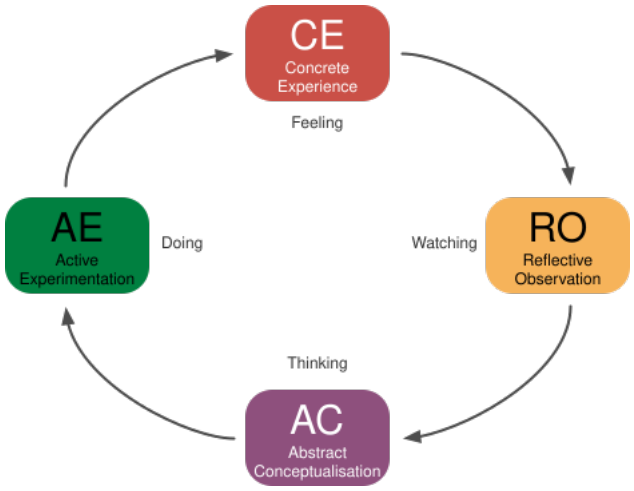


Figure 4.1: Kolb's Learning Cycle. Image Credit: [10] (Creative Commons Attribution 3.0).

4.3 Objective

Humans often represent the weakest link in any cyber system, with many advanced attacks exploiting human errors, vulnerabilities, or obvious flaws. Despite extensive research on mitigating human-related risks in cyberattacks and defense scenarios, no single model has proven entirely effective in addressing these challenges. Factors such as individual characteristics, specific environments, and the nature of the threat or defense significantly influence outcomes. In mission-critical applications, the stakes are even higher, with increased risks and associated mitigation costs.

We propose a cost-effective, programmable, and fully immersive testbed based on the DT concept, designed to simulate a mission-critical application: wastewater treatment. This platform integrates XR, AI, and DT to enhance education on cybersecurity policies and strategies. By immersing users in a realistic operational context under cyberattacks, the testbed explores scenarios where attacks exploit human errors or cybersecurity vulnerabilities. Leveraging LLMs generates motivational strategies that induce human errors, creating opportunities for further attacks. The entire process is visualized in XR to maximize user

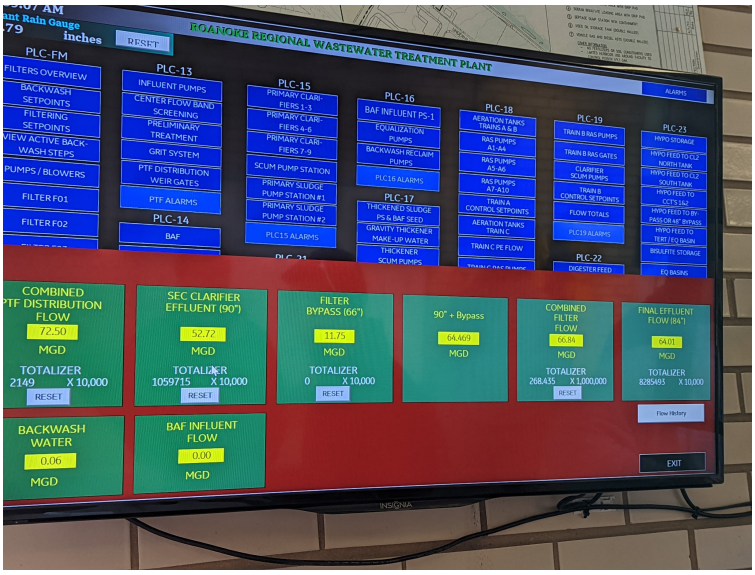
immersion and provide a realistic depiction of real-world cyberattack scenarios.

4.4 Case Study: Water Treatment Plant

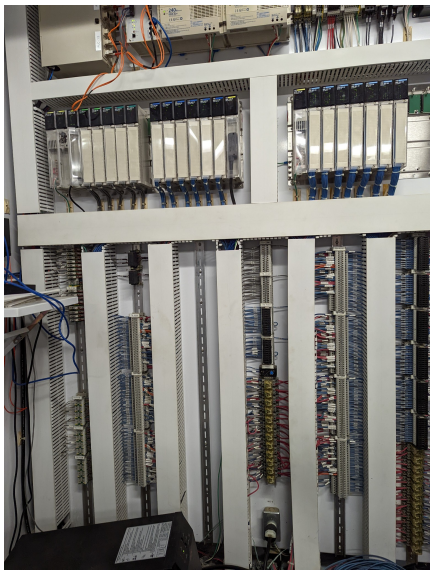
We demonstrated the implementation through a case study that provided cybersecurity education in the context of water treatment plants. We selected water treatment plants for several reasons. First, we aimed to offer training in the context of critical infrastructure to highlight the relevance of cyberattacks to all populations, regardless of an individual's background. Critical infrastructures are essential for daily life, and an attack on such systems would have far-reaching effects on everyone.

Another reason for choosing this context is that our goal was not to train users on the water treatment process but to educate them about cyberattacks. The context of a water treatment plant required minimal background knowledge compared to other types of critical infrastructure, which enabled users to better understand the scenario and focus solely on the cyberattacks themselves. Users engaged in simple tasks, such as adding or removing liquids, and then observe changes in water levels or colors to evaluate whether their actions achieved the desired results. These outcomes were self-explanatory and allowed users to interpret their observations, helping them identify potential cyberattacks based on the results without being distracted or confused by the concepts of the water treatment process.

To accurately replicate the water treatment process and gain a comprehensive understanding of the cyber-physical systems involved in its operation, we toured the Roanoke water treatment plant and interviewed workers to gather information about their cybersecurity practices and plant operations. Figure 4.2 highlights some of the key observations from the visit.



(a) UI interface at water treatment plant.



(b) Cyber physical system at a water treatment plant.

Figure 4.2: Side-by-side comparison of water treatment plant interfaces and systems.

4.4.1 System Architecture

The educational platform we proposed consisted of three main components. The first component was the **physical testbed**, which mimicked the water treatment plant on a smaller scale and provided the IoT infrastructure needed to represent the physical component of the DT concept. This IoT infrastructure enabled us to conduct cyberattacks on a real network and actual devices, eliminating the need for emulation or network simulators.

The second component was the **VR platform**, which represented the virtual side of the DT. It provided an immersive experience that simulated being at a water treatment plant, something the physical testbed could not offer. Beyond creating a realistic environment, the VR platform enhanced understanding by incorporating additional visual elements to explain concepts more effectively. The VR platform was divided into two stages: the **Tutorial Phase** and the **Practice Phase**.

- During the **Tutorial Phase**, users received an introduction to key cyberattack concepts and participated in a live demonstration.
- Once they grasped the concepts, users progressed to the **Practice Phase**, where they reinforced their learning through problem-solving activities.

To address our research questions, we used a between-subject experimental design with two distinct versions of the Practice Phase: **Non-AI guided** and **AI guided**. These versions were described in detail later in this Chapter (Section 4.4.4).

Finally, to effectively demonstrate cybersecurity principles, the platform included an **attacker agent**, who played the role of a Man-in-the-Middle attacker. This agent intercepted communication between the VR environment and the physical testbed, sabotaging the DT platform to showcase the effects of cyberattacks. We focused on teaching three types of attacks: Denial of Service, Input data manipulation, and Output data manipulation. Below, we dive into each of these components in detail and discuss how the goals were satisfied.

4.4.2 The Attacker Agent

The Attacker agent was responsible for processing requests from the VR environment to generate the appropriate attack script for the given scenario a user was in. We first received a message from the VR environment through MQTT regarding the type of attack to begin. The script then executed the appropriate attack on the relevant stage of the water treatment plant. Attack scripts were developed using Python and executed through a Kali Linux Environment. One of the main tools used was arpspoof, which is part of the dsniff suite available on Python. This tool enabled us to perform ARP Spoofing, which involved associating a different IP address with a specific MAC address. By having this functionality, we rerouted the victim's internet traffic through a computer system executing the attack

script. From there, we configured IP forwarding to either drop the packet (DOS) or forward it (Data Manipulation/Sniffing). This allowed for a Denial of Service attack (DOS) or a Data Manipulation attack to occur.

To perform sniffing or data manipulation on the intercepted packet, we used Scapy, an internet packet manipulation library, which allowed us to inspect internet traffic and filter out packets that we were not interested in. This left us with packets of relevance that we could further process. To process them, we reconfigured the iptables in Linux using Netfilter Queue (NFQUEUE) to reroute the desired packets into a queue. The program then iterated through the queue to inspect and process the packets as needed before sending them to the actual recipient.

For instance, to intercept all packets transmitting information about the current water level of a specific tank in the water treatment plant, we first executed an ARP spoofing script to redirect all packets originating from the tank's microcontroller unit to our computer. Next, we used the Scapy Python library to develop an algorithm that captured the packets of interest and employed NFQUEUE to redirect these packets to a designated area. Once intercepted, we modified the packets to report a lower water level than what was actually being read. This attack could deceive the user into believing the tank's water level was insufficient, prompting them to add more water, potentially causing an overflow.

4.4.3 Physical Testbed:

The physical testbed, designed to simulate a water treatment plant, included seven water tanks representing five distinct treatment stages. The first stage was the Primary Intake Chamber, which controlled the intake of dirty water from the sewer system. It ensured that the correct amount of water was directed into the treatment plant, preventing both overflow

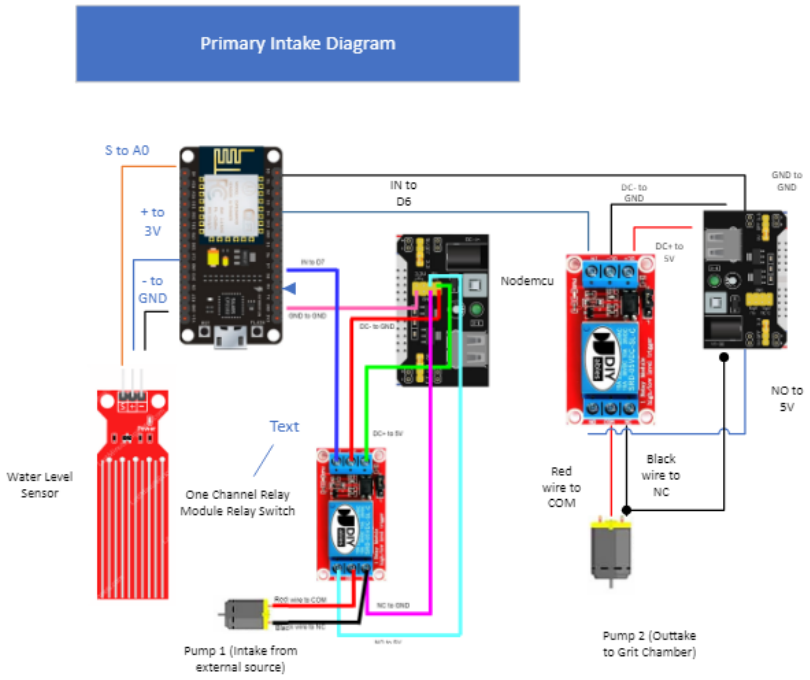


Figure 4.3: Primary intake chamber stage.

and underflow. This process optimized the system's efficiency while adhering to safety and health regulations. As shown in Figure 4.3, our stage consisted of a water level sensor to read the current water levels and two water pumps. One pump was responsible for adding more water into the chamber (intake pump), and the other pump (outtake pump) was responsible for moving the water from this chamber to the next. These components were then controlled by an Arduino NodeMCU ESP8266, which was powered by a 5 Volt power supply module.

After the Primary Intake Chamber, we moved on to the Grit Chamber (Figure 4.4), where we mimicked the removal of heavy materials from the wastewater and verified that the water quality was at an acceptable level for the next stage by using a Total Dissolved Solids (TDS) level sensor, with measurements returned in units of Parts per Million (ppm). We also had a water level sensor to ensure proper water levels. Given the limited processing power of the NodeMCU and the fact that both the TDS and water level sensors were analog, we needed to use separate NodeMCUs for each sensor to minimize the risk of failure impacting

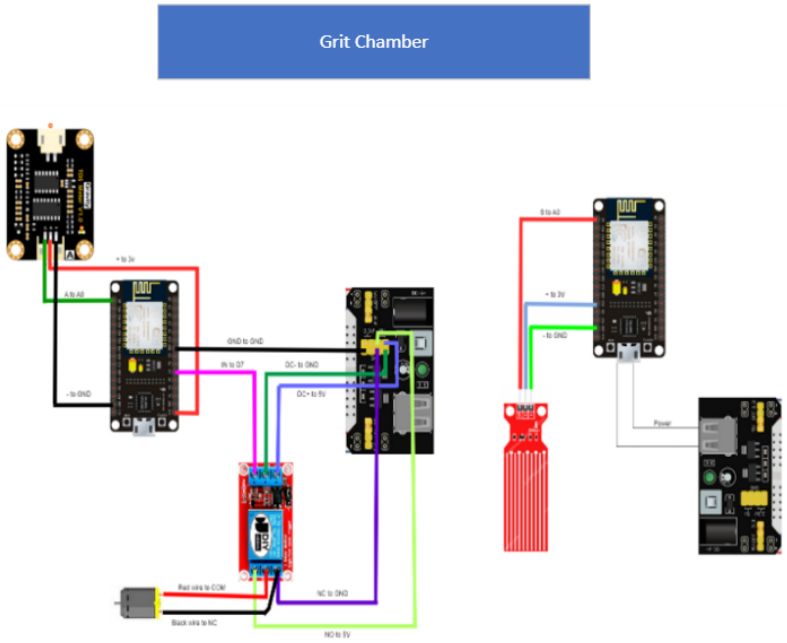


Figure 4.4: Grit chamber stage.

other components. We did, however, consider using an analog-to-digital converter (ADC) but found that it was more challenging and unreliable than expected. A water outtake pump was also included to move water from this chamber into the next. In conclusion, we found that using two separate NodeMCUs was more efficient and feasible in the long run compared to using just one.

The Chlorination Chamber (Figure 4.5) was the stage where we mimicked adding chlorine solution into the water tank to form an acidic solution. This solution allowed the dirty water to become disinfected and killed all of the harmful bacteria, making the water safer for drinking. We replaced chlorine with lemon juice, as it was considered a safer and less costly acidic solution suitable for educational purposes. The components of this stage included an Arduino MKR WiFi 1010 microcontroller, a pH level sensor, a water level sensor, and an outtake water pump. Through some experimentation, we found that the NodeMCU was incompatible with the pH level sensor, which was the reason we used the Arduino MKR

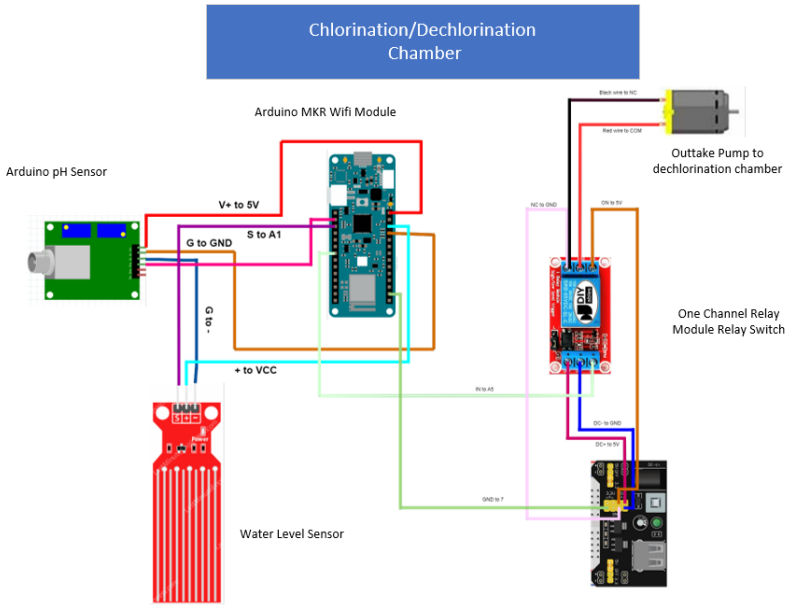


Figure 4.5: Chlorination/dechlorination chamber.

WiFi 1010 microcontroller instead.

The Dechlorination Chamber (Figure 4.5) was architecturally the same as the Chlorination Chamber. The only difference was that we used a basic compound instead of an acidic compound, as we wanted to reverse the chlorination effect. To represent the basic compound, we used window cleaner fluid.

The final stage was the Quality Monitoring Chamber (Figure 4.6), where we ensured that the fresh drinking water met all standards before we introduced it back into the surrounding environment. To verify the water characteristics, we included a pH level sensor, a water level sensor, and a water temperature sensor. The final result of the testbed can be seen in Figures 4.7 and 4.8.

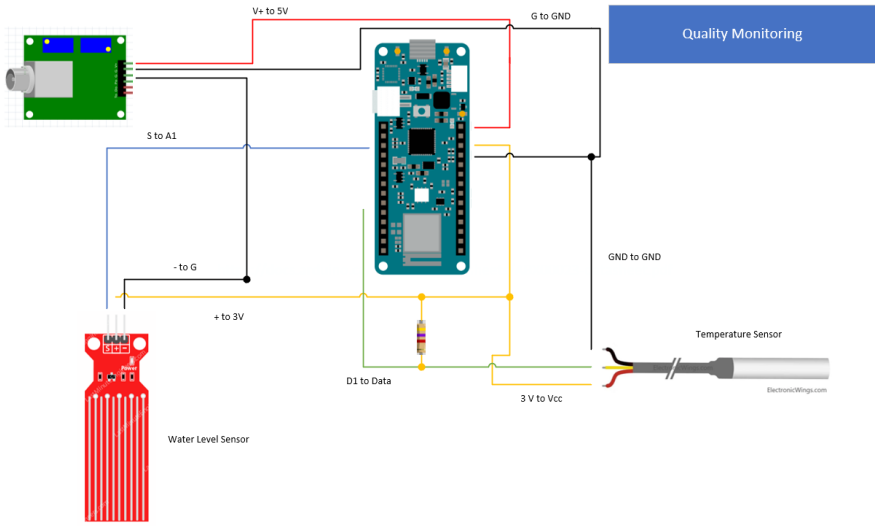


Figure 4.6: Quality monitoring chamber.

Figure 4.7: Top down view of testbed.

Figure 4.8: Front view of testbed.

4.4.4 VR Environment

Our VR Environment was developed using Unity 2022.3.20f and the C# programming language. For running the application, we used the Meta Quest 2 (Figure 4.9). We broke our VR system into three major components: the Tutorial Phase, the Practice Phase without AI Guidance, and the Practice Phase with AI Guidance. We aimed to investigate how AI could be used in conjunction with the DT Concept and VR for educational purposes. The two different practice phases allowed us to conduct a between-subjects user study, where we compared the learning effects of AI-guided versus non-AI-guided learning.

Tutorial Phase

The tutorial phase allowed users to become acquainted with the VR environment and learn about the three cyberattacks. This achieved the first two stages of the experiential learning

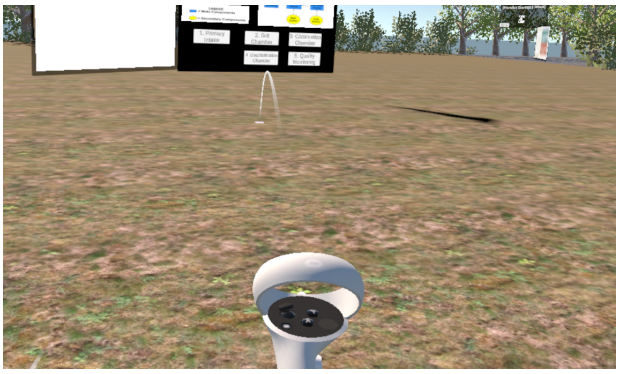
Figure 4.9: Meta Quest 2 VR HMD.

cycle (Concrete Experience and Reflective Observation). To do this, we used a combination of audio narration and a set of guided tasks. The user was welcomed into the environment and explained the overall purpose of the VR application. The program then guided the user through the basic controls, such as the moving mechanism and how to interact with the UI within the virtual environment (Figure 4.10a). We used teleportation in our system as it prevented users from experiencing VR motion sickness compared to virtual walking and ensured they focused only on proceeding to the desired areas (Figure 4.10b). After users became familiar with the controls, they proceeded to learn about the stages involved in water treatment plants. This process involved a lecture provided through an audio narration and associated slides when users selected the appropriate button (Figures 4.11a and 4.11b).

After that, the users experienced the three different cyberattacks. During this stage, participants received an audio narration explaining the attack (Figures 4.12a and 4.12b), after which they interacted with the water tank to familiarize themselves with its controls and basic functions. As they proceeded with the tutorial, they activated the cyberattack and saw how it affected the functionality of the water tank (Figure 4.12c). Hence, providing the users a comparison of what happened normally and how its functionality changed with a

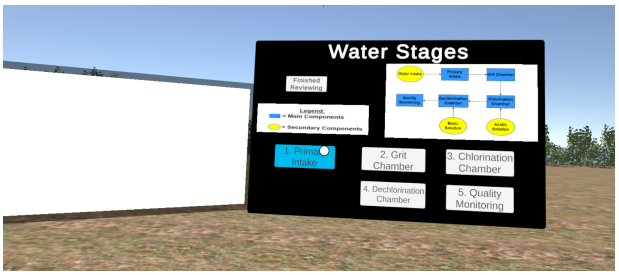
specific cyberattack. Once users completed all three of the cyberattack tutorials, they were ready to proceed to one of the two practice phases, which were randomly selected for them.

(a) VR tutorial phase: controller tutorial.

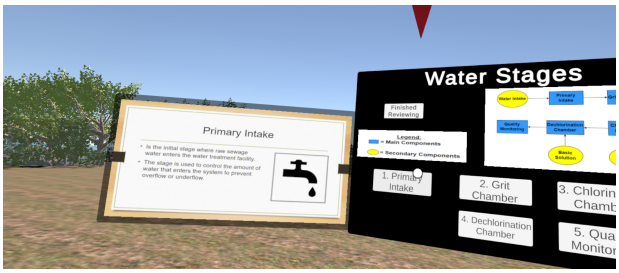


(b) VR teleportation mechanism.

Figure 4.10: Controller tutorial features.



(a) Water stage navigation buttons.

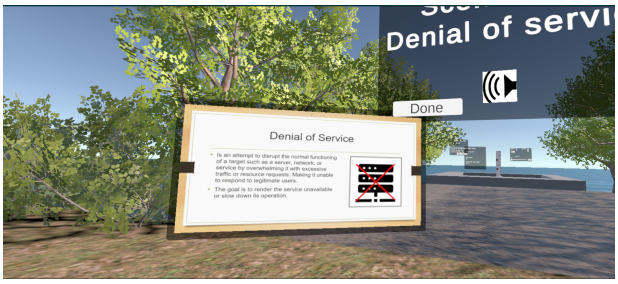


(b) Water Stage Lecture Slide.

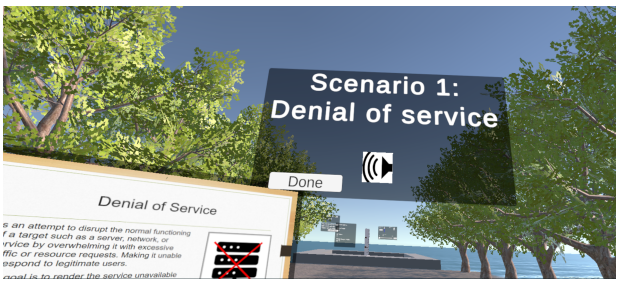
Figure 4.11: VR tutorial phase: water stage learning section.

Practice Phase

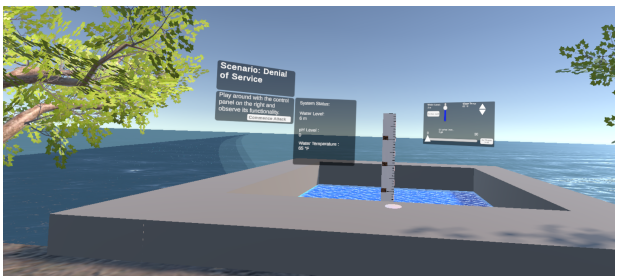
In the Practice Phase, users went through six scenarios where they were tasked with performing a normal water treatment operation. However, as they proceeded to do so, they may or may not have experienced the occurrence of a cyberattack. While going through these six stages, users were responsible for determining if a cyberattack had occurred and then classifying it. This achieved the Abstract Conceptualization and Active Experimentation stages of the learning cycle. During this phase, users interacted with the hardware



(a) Denial of service lecture slide.



(b) Denial of service panel.



(c) Water Tank Demo.

Figure 4.12: VR tutorial phase: cyberattack lesson - denial of service.

component through the VR environment. In other words, any actions they performed in the VR environment were reflected in reality. Users could then verify if tasks were completed successfully with access to a set of cameras used to monitor changes in the physical counterpart of the DT. This tool allowed them to verify if their actions in the virtual environment had the correct effect on their physical counterparts. We provided the details of the five scenarios users completed below:

Scenario 1

- **Tank Stage**: Primary Intake
- **Task Objective**: Ask the user to increase the water level by turning on the intake pump.
- **Attack Type**: Input Data Manipulation – Users attempt to add more water into the

chamber, but instead, the outtake pump (removing the water from the chamber) will turn on. Users see that the water level does not increase through the web camera.

Scenario 2

- **Tank Stage**: Grit Chamber
- **Task Objective**: Ask the user to remove some water from this chamber and move it to the Chlorination chamber.
- **Attack Type**: Denial of Service – Users see that when they attempt to turn on the outtake pump, it does not respond to their controls.

Scenario 3

- **Tank Stage**: Chlorination Chamber
- **Task Objective**: Ask the user to add some acidic solution to decrease the pH level.
- **Attack Type**: Output Data Manipulation – Users see the pH level increase while trying to decrease it and notice that it is not possible since it is completely disconnected from the basic solutions chamber. They also see that there is water movement inside the Chlorination Chamber through the camera due to acidic solution being added.

Scenario 4

- **Tank Stage**: Dechlorination Chamber
- **Task Objective**: Ask the user to add some basic solution to increase the pH level.
- **Attack Type**: None. Users see normal behavior: pH level increases as expected.

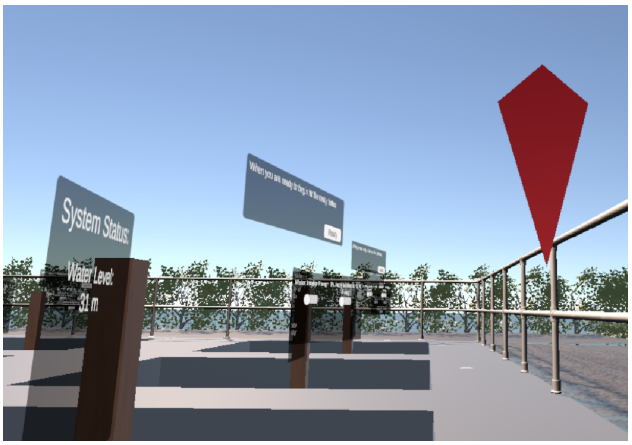


Figure 4.13: Red arrow indicating to users where to proceed

Scenario 5

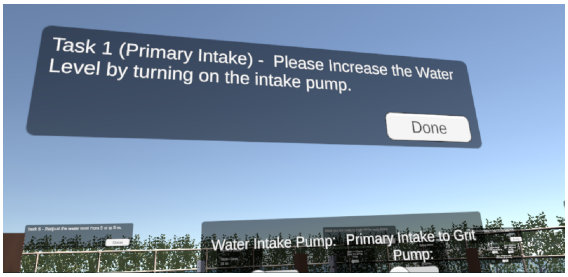
- **Tank Stage**: Quality Monitoring Chamber
- **Task Objective**: Ask the user to add some water to the tank.
- **Attack Type**: Denial of Service – Users see that the water level sensor output does not change and verify through the camera that there is no water movement flow.

Non AI Guided Version

In the Non-AI guided version of the practice phase, users were guided through voice narration prompts just like in the tutorial. Red arrows indicated to the users where to teleport as they made progress (Figure 4.13). Once users were ready to begin, they could hit the ready button presented to them, and activating the button began the cyberattack script on the back end (Figure 4.14). At this time, a prompt and audio narration popped up, providing the users with a task to complete. Once users had attempted to complete the task and were ready to provide an answer, they could simply select the done button (Figure 4.15a). The user used a drop-down menu within the VR environment to select the appropriate answer

Figure 4.14: User interface at a given scenario for non-AI practice phase.

for the cyberattack they had just experienced (Figure 4.15b). Based on the answer selection, feedback was provided to the user, informing them if they had selected the correct answer or not, along with a brief explanation (Figures 4.16a and 4.16b).



(a) Task instructions.

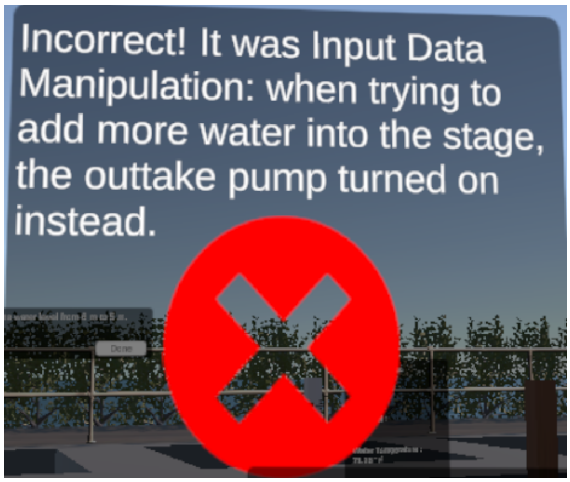
(b) Drop-down menu to provide answer.

Figure 4.15: Instruction and answer selection for VR non-AI guided task.

AI Guided Version

In the AI-guided version of the practice phase, we used a Unity asset known as Convai [21]. This enabled a fully interactive NPC character to be present in the virtual environment, allowing users to ask questions and receive answers. In other words, it was like there was a real person with them, guiding them through the process. Users were able to communicate with the AI NPC through Push-to-Talk speech-to-text recognition. This asset utilized the ChatGPT-4o LLM as its core engine to generate dynamic and engaging responses. Convai also featured a Narrative Design functionality, which allowed us to program a sequence of

(a) Correct answer feedback.



(b) Incorrect answer feedback.

Figure 4.16: Feedback for correct and incorrect answers in the VR non-AI guided scenario.

actions for the AI character to narrate a story (Figure 4.17). The role of the AI character was to guide users through each scenario, creating the sensation that a real person was accompanying them and walking them through each step of the experience. This replaced the voice narration and drop-down menu feature that the Non-AI Guided version had, as the AI character could handle both functionalities in a more natural and engaging form. Figure 4.18 demonstrated how an AI NPC introduced the user to the scenario and gave them the task to complete.

When users approached the AI NPC character, the NPC automatically greeted the user. This was done by using the concept of triggers in the Unity development environment that detected when two game objects collided with each other. This was a key feature in our program as it allowed the AI to talk to the users at the right moment when they were being guided through the scenarios. In addition, the AI NPC character could walk around within the VR environment, allowing users to be guided on where to proceed throughout the Practice phase (Figure 4.19).

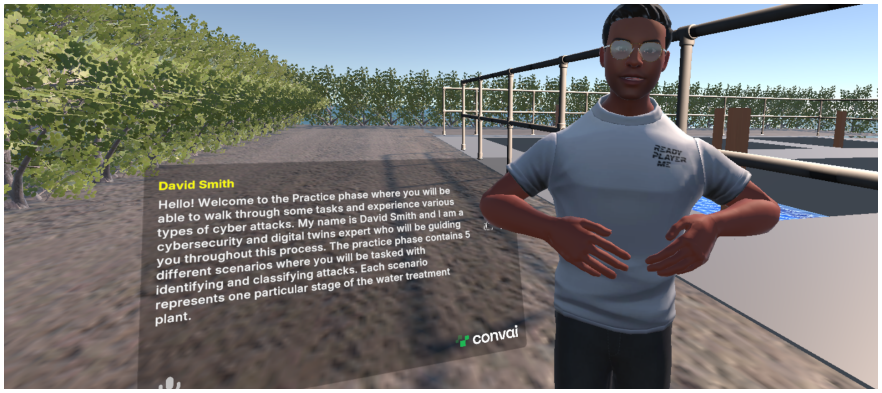


Figure 4.17: Convai character giving introduction to user.

Figure 4.18: Convai character introducing the first scenario.

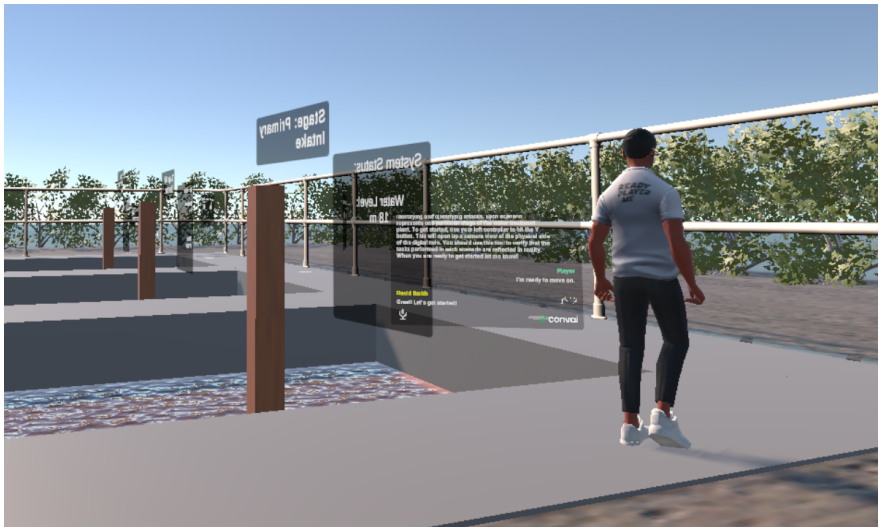


Figure 4.19: Convai character walking user to scenario.

4.4.5 The MQTT Connection

Our VR environment (the digital part of the DT) aimed to provide an immersive user interface for the hardware side. To achieve this, we established a communication link to the hardware testbed through a communication protocol called Message Queuing Telemetry Transport (MQTT). The MQTT architecture consisted of three components: a broker, a topic, and a message. The broker served as the host/server where all MQTT messages went through to reach the other users. We utilized an MQTT broker, hosted via Home Assistant, a widely-used open-source platform for smart home integration. It ran on a Raspberry Pi 5. All devices communicated with this broker to either send a message (publish) or listen to and receive messages (subscribe). When communicating through MQTT, communication channels were established using topics, which consisted of a unique string. All MQTT packets that shared that unique string spoke on the same channel. Attached was also the message component, which contained the actual data that wanted to be sent to the other parties.

The MQTT architecture was configured so that each hardware component in every stage operated on its own dedicated channel. This ensured that communication for each component remained independent and prevented any interference between them.

Chapter 5

Study Design

In this section, we describe the layout of the user study conducted and dive into what users will be doing and the reasoning behind each step. The procedures for the user study are then presented. We also present our hypotheses for the research questions we introduce.

The study is conducted using a between-subject design approach where participants are randomly assigned to one of two groups. This helped us answer research question two described in Section 1.3.2. The two groups are the following:

1. AI Guided Learning

2. Non-AI Learning (Self-Guided Walkthrough)

Both groups performed identical tasks in the tutorial and practice phases. The only difference between the two groups was the modalities with which the users were presented during the practice phase. Users in the AI group conversed with an AI NPC throughout the Practice Phase, while Non-AI users simply interacted with various UI elements.

Users were first asked to fill out a pre-study survey that asked them about their demographics and background with cybersecurity and VR concepts. They were then asked to take a cybersecurity assessment where we collected knowledge on their current level of cybersecurity understanding. The cybersecurity assessment contained 9 different questions testing them on their knowledge of denial of service, input data manipulation, and output data manipulation

attacks. Each question was worth one point, and we used this data to calculate the score difference between the after-study score and the before-study score. We then used the scores from the two groups to compare them and see if there was a statistical difference.

During the study, users underwent two phases, the first one being the tutorial phase. Here, users learned how to navigate the VR environment, interact with the UI, and learn about the three different cyberattacks: Denial of Service, Input Data Manipulation, and Output Data Manipulation. During the learning process, users had an opportunity to become familiar with the functionalities of the water treatment plant control panel and also experienced the attack. By allowing the users to learn about the attack and then experience the characteristics of the attack firsthand, we supported the first two stages of Kolb's Experiential Learning Cycle, which were Concrete Experience and Reflective Observation. Once completed, users moved onto the practice phase, where they were given five different tasks to complete related to wastewater treatment and then asked to identify and classify any cyberattacks they encountered. During this phase, users verified that actions performed in the virtual environment matched what happened on the physical side of the DT by viewing its status information and observing the physical system through a web camera. This supported the Abstract Conceptualization and Active Experimentation stages of the learning cycle through encountering experiences.

There were two possible scenarios for the practice phase: AI-guided learning and Non-AI-guided learning. Users undergoing the AI practice phase interacted with an AI character that guided them through the scenarios. Participants were able to provide their answers to this character and also ask any questions they had through conversation. The Non-AI participants were guided through text and audio narration prompts along with visual markers.

Following the study, users were asked to complete the same cybersecurity assessment again

to see if they improved after learning about the concepts through the platform. In addition, users were asked to complete a post-study survey that gathered data on their experience with the system. We focused on obtaining data regarding the system's usability, their feeling of presence while using the system, and the workload they encountered. Details of how we obtained this data were presented in the next chapter. Participants also took part in an exit interview to identify desired features, elements that supported learning, and areas in need of improvement.

Below were the procedures used to conduct the user study:

1. The participant arrived and was provided with an overview of the user study and what they would be doing.
2. The participant reviewed and signed the consent form with the user study staff. Any questions the participant may have had was answered.
3. Participants then filled out a pre-study questionnaire to gauge demographics and then took the pre-study cybersecurity assessment.
4. Users then were instructed on the basic VR controls for our platform and then asked to put on the VR headset.
5. Users completed the tutorial phase of the VR program.
6. Then the user moved on to complete the practice phase.
7. Once users finished the practice phase, participants then were asked to take the post study cybersecurity assessment.
8. Users then be asked to fill out a survey regarding their experience and asked a series of questions through an exit interview.

The procedure above took around 1 hour to complete.

5.1 Hypothesis

Using the two research questions (Sections 1.3.1 and 1.3.2), we generated the appropriate hypothesis. Research Question 1 focused on the impact of combining a virtual environment with a physical environment for learning purposes. Research Question 2 focused on whether AI-guided learning had an impact on learning outcomes and experiences. We proposed the two hypotheses below:

1. H1: Using a VR DT-based platform for cybersecurity education will enhance knowledge retention about cyberattacks and improve the interpretation of system behavior by leveraging insights from the physical environment.

2. H2: AI Guided Learning will prove to have a higher learning improvement score and higher experience ratings than the non-AI learning group.

Chapter 6

Results

This chapter presents the results from both the pilot study and the user study. It begins with the findings from the pilot study where we detail the identified issues and the measures taken to address them. Next, the chapter provides details of the user study results, including demographic information about the participant pool, a description of the key factors analyzed, the methods used to calculate them, and the statistical analyses employed to interpret the findings. Qualitative results from the exit interviews are also presented, highlighting features that were effective, those that supported learning, and areas requiring improvement.

6.1 Pilot Study Results

A pilot study was conducted with 6 participants where 3 participated in the AI guided learning while 3 participated in the Non-AI guided learning. The population consisted of 3 males and 3 females. The pilot study provided qualitative feedback to help improve usability and clarity for users. Several bugs were also identified during this process.

A significant flaw discovered during the pilot study was that the teleportation anchors within the environment were more challenging to use than expected. The teleportation anchors were intended to restrict users to specific areas within the VR environment. However, since most participants were inexperienced with VR and lacked precise hand movements, they found

the teleportation anchors difficult to use. To address this, the teleportation mechanism was improved by enlarging the target area and accommodating less precise hand movements.

For participants who were a part of the AI-guided group, the AI NPC character had issues regarding its movement to the appropriate water tanks that the users followed. In many instances, the AI NPC would not move to the correct spot precisely and would be located too close to the user making them feel uncomfortable. Hence, the AI NPC's movements were further refined to alleviate this issue. It was also observed during the pilot study that the AI would inform the users that their answers were correct when they were completely wrong. This was due to the lack of precision and contextual information provided to the AI NPC. Refinement was achieved by training the AI with examples of incorrect answers and examples of correct answers. This helped restricting its decision-making to the important keywords found in the correct answers.

These were the two most significant issues identified during the pilot study. Other smaller issues were primarily related to the User Interface layout and flow, as participants found some elements unclear and in need of further clarification.

6.2 Study Results

This section outlines the results of the user study. We conducted a between-subject study comparing two groups: AI-guided and non-AI guided learning. A total of 36 participants were randomly assigned to one of the two groups, with 18 participants in the AI-guided learning group and 18 in the Non-AI guided learning group. The G* Power tool was used to calculate the appropriate amount of participants needed. All participants completed identical pre and post-study surveys and underwent the same tutorial phase. Unfortunately, we had to exclude data from two participants: one experienced severe motion sickness, and the other

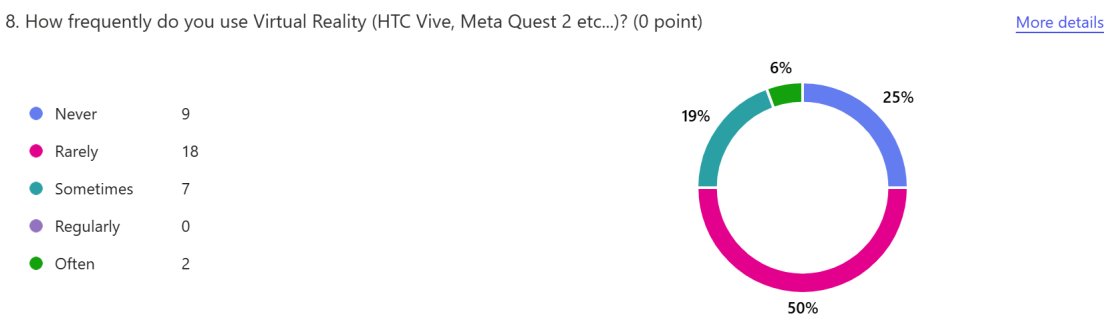


Figure 6.1: VR usage demographics.

encountered an unexpected failure of the AI LLM. Statistical analyses were performed using JMP Pro 16 software.

6.2.1 Demographics

The demographics of the participant population consisted of undergraduate and graduate Virginia Tech students who primarily majored in Computer Science. There were some students from Industrial and Systems Engineering, Biochemistry, and Psychology as well. All participants were at least 18 years of age or older as required by the IRB protocol. The age group ranged from 18 years to 38 years old and there were 11 female and 25 male participants.

Most participants have limited experience in utilizing VR platforms (Figure 6.1), suggesting a significant learning curve for adapting to this type of system for educational purposes. Additionally, participants show limited knowledge of cyberattacks and the DT concepts (Figures 6.2 and 6.3). This offers an ideal population for evaluating our platform's effectiveness in engaging and educating novice users.

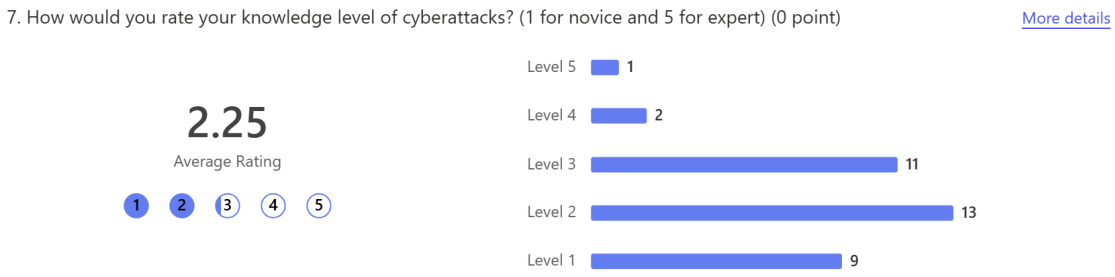


Figure 6.2: Participant cyberattack knowledge.

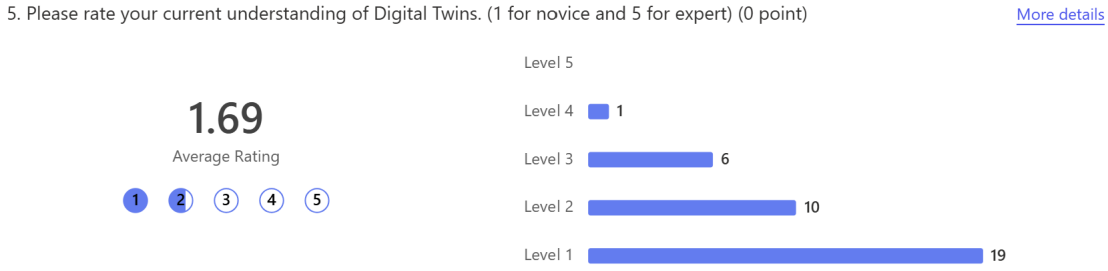


Figure 6.3: Participant DT knowledge.

6.2.2 Learning Improvement

Between Group Comparison

In this section, we focus on comparing learning improvement between the AI-guided group and the non-AI group. To measure learning improvement, users were asked to take a cybersecurity assessment before and after the study. We used these two scores as a comparison to see if they have improved or not. Users were presented with 9 questions worth one point each for a maximum of 9 points. Table 6.1 presents the raw average scores from the cybersecurity assessment completed by participants both before and after the study for each group as well as each group's improvement score.

Table 6.1: Average Cybersecurity Assessment Scores

Modality	Pre Scores	Post Scores	Improvement Scores
AI Guided	5.55	7.11	1.55
Non AI Guided	5.44	7.72	2.27

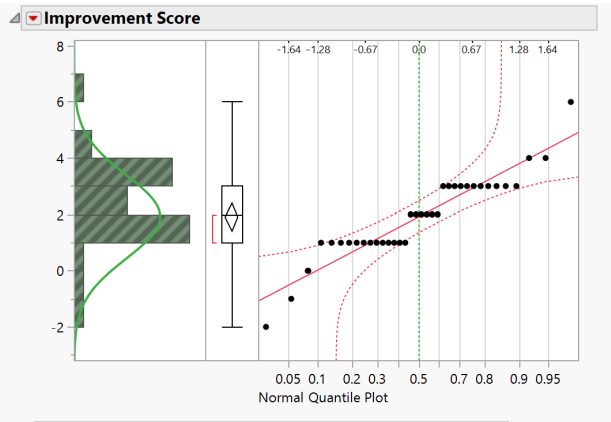
Normality Testing of the Data We initially considered using a two-sample t-test statistical analysis to determine if the mean score values between the two groups had any significance in their difference. Our two populations met the criteria of being independent of each other. In addition, participants were randomly selected into AI or non-AI guided learning groups using systematic random sampling which satisfies the random sampling criteria. However, when plotting the data on a histogram and Normal Quantile Plot, it showed that the data did not possess the normality characteristic (Figure 6.4). This is important as we need to know what kind of statistical analysis is appropriate for the data we have obtained. In addition, we ran the Shapiro-Wilk test for normality. We obtained a p-value of 0.0095 which is less than the significant level of 0.05. Therefore we reject the null hypothesis and see that there is statistical evidence that the dataset does not follow a normal distribution. Hence, we can no longer use a two-sample t-test. Instead, we use the Wilcoxon rank-sum test, also known as the Mann-Whitney U test, to perform our statistical analysis, as it does not require normality in the data.

Statistical Comparison We use the following hypothesis format for all calculations in the following sections. The null hypothesis is that the mean scores for the two groups (S_a and S_b) are the same. For this particular analysis, the scores from the AI-guided learning group (S_a) are the same as the scores from the non-AI guided group (S_b). In other words, the null hypothesis (H_0) and alternative hypothesis (H_1) are as follows:

$$H_0 : S_a = S_b$$

$$H_a : S_a \neq S_b$$

The analysis here will help us answer RQ2 (Section 1.3.2) and see if AI agents have an impact on learning or not.



(a) Learning improvement data plot.

Fitted Normal Distribution

Parameter		Estimate	Std Error	Lower 95%	Upper 95%
Location	μ	1.9166667	0.246805	1.4329378	2.4003955
Dispersion	σ	1.4808299	0.1464968	1.2198229	1.5619831

Measures	
-2*LogLikelihood	129.43097
AICc	133.7946
BIC	136.598

Goodness-of-Fit Test

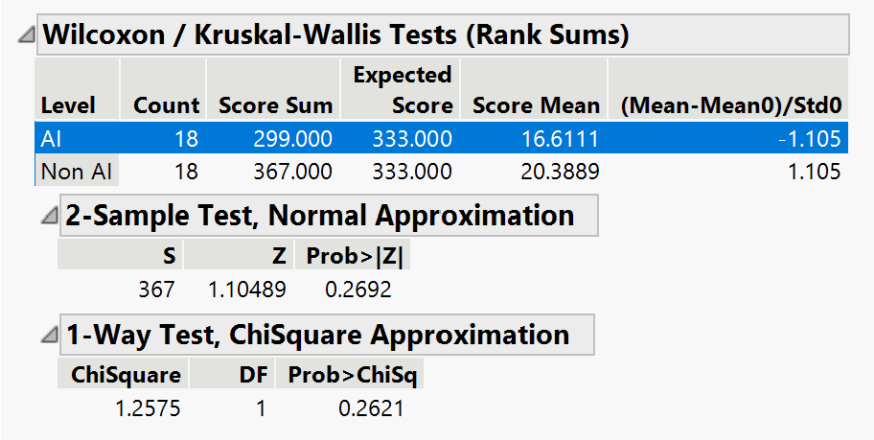
	W	Prob<W
Shapiro-Wilk	0.9157378	0.0095*

	A2	Simulated p-Value
Anderson-Darling	1.4062558	<.0001*

(b) Learning improvement Shapiro-Wilk test result.

Figure 6.4: Learning Test for Normality Results.

We can see from the results (Figure 6.5) that by conducting the Wilcoxon Rank Sums test on the learning improvement score, we obtained a p-value of 0.2692 which is larger than the significant level of 0.05. We also see that the Z score is very close to 0 which indicates that there is no meaningful difference in scores here despite the improvement scores for Non-AI being better than the AI group's scores. We also analyzed our results using a 1-way Chi-Square approximation and can confirm here that the p-value of 0.2621 proves there is no significant difference between the two groups. Hence, we fail to reject the null hypothesis and conclude that having AI Agents does not affect the learning outcomes. This is further supported by figure 6.6 where we can see the box plots for AI and Non-AI groups side by side. The overlap is pretty significant which supports that there is no statistical difference in learning improvement between the two. However, we did notice some low data points for



Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
AI	18	299.000	333.000	16.6111	-1.105
Non AI	18	367.000	333.000	20.3889	1.105

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
367	1.10489	0.2692

1-Way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
1.2575	1	0.2621

Figure 6.5: Learning Wilcoxon Rank Sums test results.

the AI group and high data points for non-AI group. We discuss this further in the next chapter (Chapter 7).

General Learning Improvement

This section analyzes if the developed platform provides a general learning improvement in cybersecurity concepts across the board. To do this, we compare the pre and post-test scores from all participants regardless of their assigned group.

Normality Testing of the Data We use the same set of tests and observations to determine if the data we received is considered normal. We see from the Normal Quantile plot that the data does not demonstrate normal behavior (Figure 6.7a). To further support this conclusion, we obtain a p-value of 0.0005 from the Shapiro-Wilk test (Figure 6.7b). Hence we reject the null hypothesis and conclude that the data is not normally distributed.

Statistical Comparison Proceeding with the Wilcoxon Rank Sums test (Figure 6.8), we see a p-value of less than 0.001 which is significantly less than the significant value of

Figure 6.6: Learning improvement box plot.

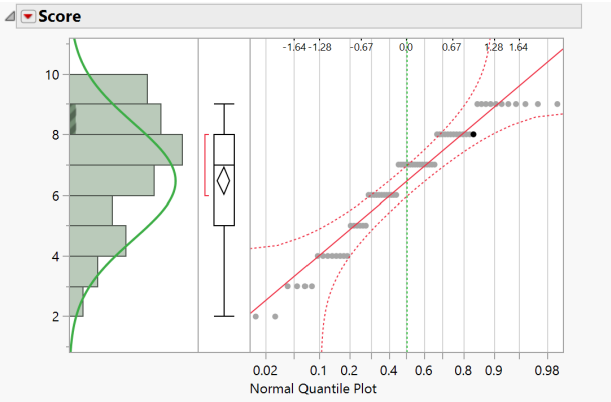
0.05. Hence, we can conclude here that the pre and post-study cybersecurity test score are statistically different. Meaning that our platform on average improves cybersecurity knowledge effectively for all participants.

6.2.3 User Satisfaction

To measure various factors for user satisfaction, we measure three different characteristics: system usability, workload, and presence. The results for the characteristics are shown in Table 6.2.

Table 6.2: Average User Satisfaction Scores based on Modalities

Modality	SUS (out of 100)	Workload (out of 100)	Presence (out of 5)
AI Guided	78.75	34.69	3.26
Non AI Guided	81.94	33.31	2.99



(a) General learning data plot.

Fitted Normal Distribution

Parameter		Estimate	Std Error	Lower 95%	Upper 95%
Location	μ	6.4583333	0.2245997	6.018126	6.8985407
Dispersion	σ	1.9057918	0.1162594	1.6910226	1.9573164

Measures	
-2*LogLikelihood	296.1924
AICc	300.36631
BIC	304.74573

Goodness-of-Fit Test

	W	Prob<W
Shapiro-Wilk	0.9282422	0.0005*

	A2	Simulated p-Value
Anderson-Darling	1.6609425	<.0001*

(b) General learning Shapiro-Wilk test result.

Figure 6.7: General learning test for Normality results.

Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
Post Study	36	1690.00	1314.00	46.9444	4.287
Pre Study	36	938.000	1314.00	26.0556	-4.287

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
938	-4.28729	<.0001*

1-Way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
18.4298	1	<.0001*

Figure 6.8: General learning Wilcoxon Rank Sums Test results.

System Usability (SUS)

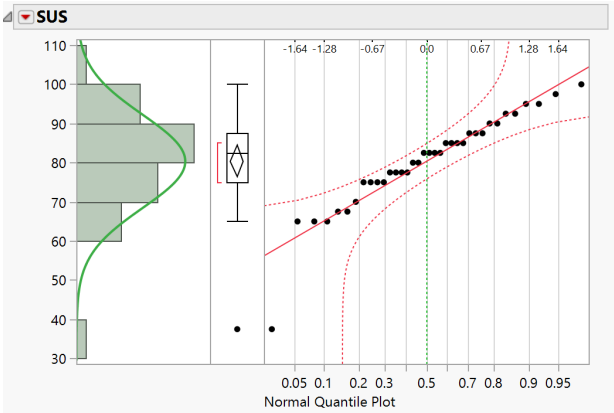
To measure system usability, we used a well-known standard for the Human-Computer Interaction community known as the system usability scale (SUS) [28]. The SUS consists of 10 questions in which users are asked to rate their agreement with each statement on a scale from 1 (strongly disagree) to 5 (strongly agree). Once we have the results, we use the following equations to calculate the SUS score where (q_i) represents the ith question:

$$x = \left(\sum_{\text{odd}} q_i\right) - 5$$

$$y = 25 - \left(\sum_{\text{even}} q_i\right)$$

$$\textbf{SUS Score} = (x + y) * 2.5$$

Once all SUS scores have been calculated, we plot the data and perform the Shapiro-Wilk test to test for normality (Figure 6.9).



(a) SUS data plot.

Fitted Normal Distribution

Parameter		Estimate	Std Error	Lower 95%	Upper 95%
Location	μ	80.347222	1.9874427	76.451906	84.242538
Dispersion	σ	11.924656	0.4157176	11.137078	12.578158

Measures	
-2*LogLikelihood	279.62336
AICc	283.987
BIC	286.7904

Goodness-of-Fit Test

	W	Prob<W
Shapiro-Wilk	0.919382	0.0121*

	A2	Simulated p-Value
Anderson-Darling	0.5500091	0.1576

(b) SUS Shapiro-Wilk test result.

Figure 6.9: SUS test for normality results.

Normality Testing of the Data Based on the test results, the p-value of 0.0121 is less than our significance level of 0.05. Therefore, we reject the null hypothesis and conclude that the data does not follow a normal distribution.

Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
AI	18	294.000	333.000	16.3333	-1.222
Non AI	18	372.000	333.000	20.6667	1.222

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
372	1.22226	0.2216

1-Way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
1.5330	1	0.2157

Figure 6.10: SUS Wilcoxon Rank Sums test results.

Statistical Comparison We then proceed to use the Wilcoxon Rank Sums test (Figure 6.10) to determine that we get a p-value of 0.2216 and a Z value of 1.22226. Hence, we fail to reject the null hypothesis in this case and conclude that the SUS averages between the two groups are not statistically different at the significance level of 5%. From the box plot in figure 6.11, the AI group's results exhibit a greater spread compared to the Non-AI group, indicating higher variability in usability among participants interacting with the AI LLM. We discuss some theories as to why this spread occurs in Section 7.1.2.

Presence

For presence, we used the iGroup Presence Questionnaire [38]. The questionnaire includes 13 agreement statements, where participants rate their level of agreement on a 5-point scale. 1 represents Strongly Disagree and 5 represents Strongly Agree.

Normality Testing of the Data The p-value of 0.0939 indicates that we fail to reject the null hypothesis, suggesting that the data could be normally distributed. Additionally, the Normal Quantile plot supports this conclusion, as it shows that the data is largely consistent

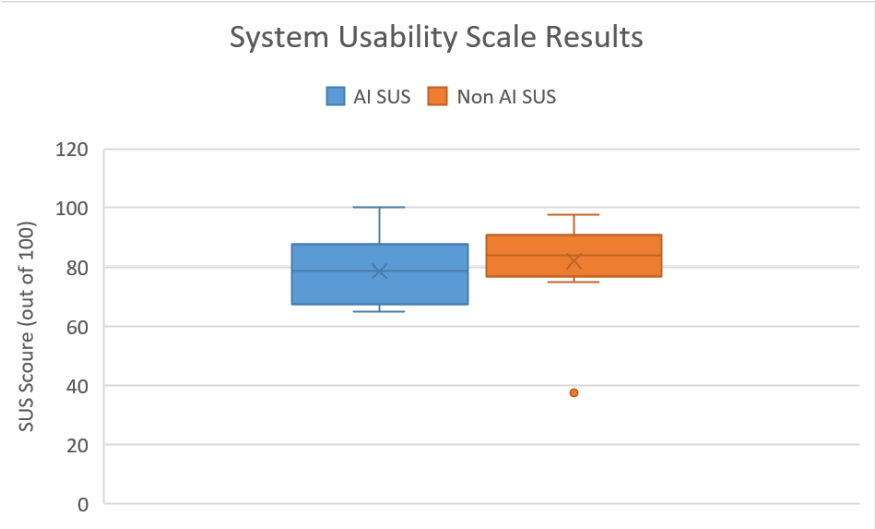
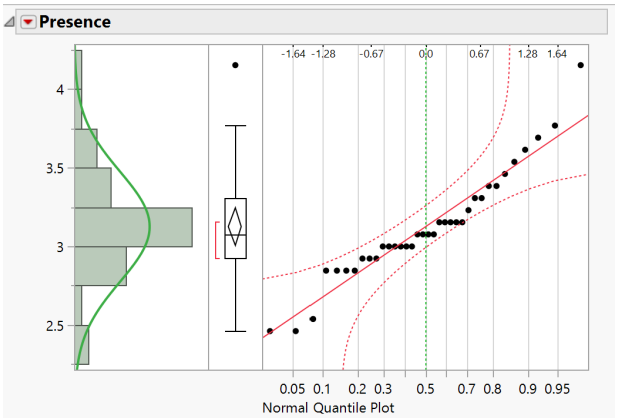
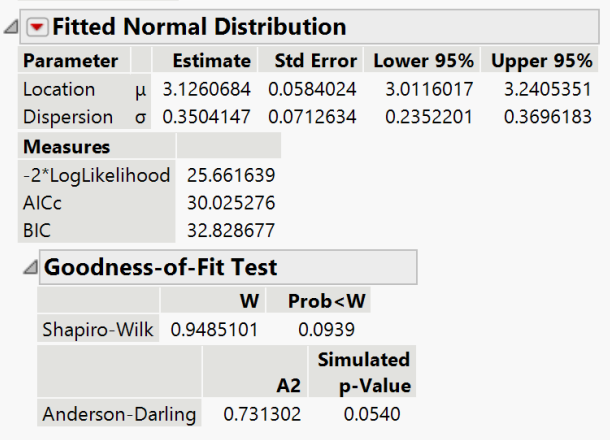


Figure 6.11: SUS box plot.

with normal distribution. Therefore, we proceeded with a pooled (two-sample) t-test.



(a) Presence data plot.



Fitted Normal Distribution

Parameter		Estimate	Std Error	Lower 95%	Upper 95%
Location	μ	3.1260684	0.0584024	3.0116017	3.2405351
Dispersion	σ	0.3504147	0.0712634	0.2352201	0.3696183

Measures	
-2*LogLikelihood	25.661639
AICc	30.025276
BIC	32.828677

Goodness-of-Fit Test

	W	Prob<W
Shapiro-Wilk	0.9485101	0.0939

	A2	Simulated p-Value
Anderson-Darling	0.731302	0.0540

(b) Presence Shapiro-Wilk test result.

Figure 6.12: Presence test for normality results

Statistical Comparison The results from the Pooled t-test (Figure 6.13) show that we obtained a p-value of 0.0233 which is less than the significant level of 0.05. We reject the null hypothesis and see that there is a statistically significant difference in presence between the AI group and the non-AI group. AI-guided learning is seen to have higher levels of presence

compared to non-AI guided learning.

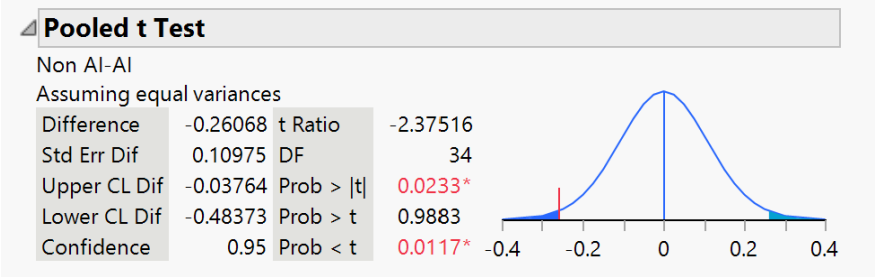


Figure 6.13: Presence Pooled t-test test results.

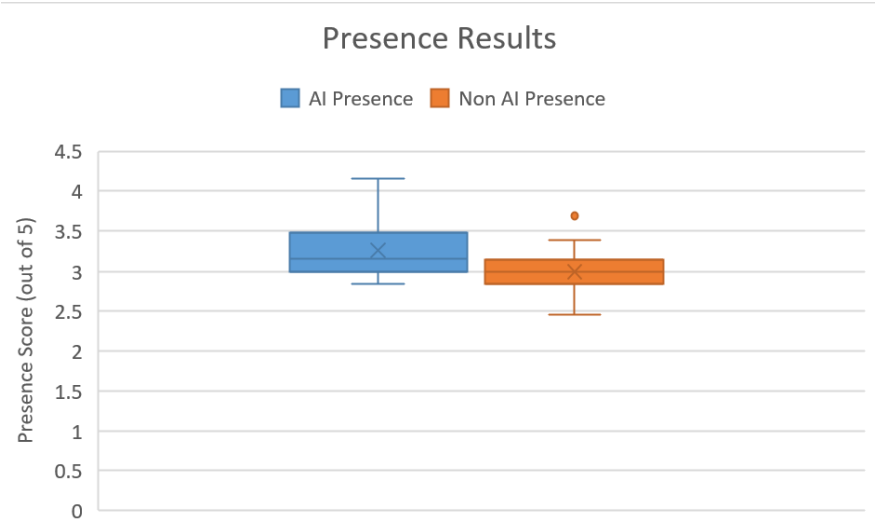


Figure 6.14: Presence box plot.

Workload

To measure workload, we used the standardized NASA Task Load Index [5] which consists of 6 questions covering the following characteristics:

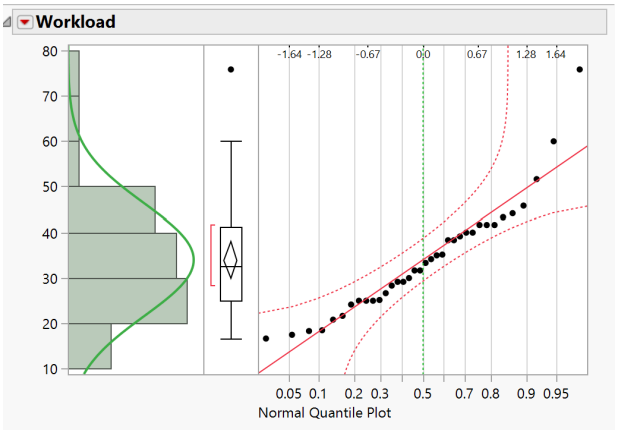
- Mental Demand
- Physical Demand
- Temporal Demand

- Performance
- Effort
- Frustration

When filling out the NASA TLX form, users were asked to provide a rating for each question from 0 to 100 to provide how much mental, physical, and temporal workload they experienced, as well as their perceived effort, performance, and frustration levels during the task. In the NASA TLX, a rating of 0 indicates that the user did not experience that factor, while a rating of 100 signifies they experienced an extreme level of that factor in the given category. This approach effectively evaluated the user's workload while interacting with our system and helps identify areas for improvement.

Normality Testing of the Data We saw from Figure 6.15b that we rejected the null hypothesis and concluded that the workload data we obtained was not normally distributed, as we obtained a p-value of 0.0113 from the Shapiro-Wilk test. We also looked at the data plot in Figure 6.15a and observed that it suggested the non-normality of the data. Therefore, we conducted the Wilcoxon Rank Sums test to analyze if there were any significant differences in workload between the two groups.

Statistical Comparison We performed a Wilcoxon Rank Sums test (Figure 6.16) and obtained a p-value of 0.5474. Hence, we failed to reject the null hypothesis, concluding that even though the workload average was higher for the AI group, there was no significant difference between the two populations. Therefore, the workload scores were considered to be the same. The box plot shown in Figure 6.17 also supported this, as the box plot showed that the majority of scores overlapped between the two groups. We discussed later



(a) NASA TLX Data Plot.

Fitted Normal Distribution

Parameter		Estimate	Std Error	Lower 95%	Upper 95%
Location	μ	33.996389	2.0596362	29.959576	38.033202
Dispersion	σ	12.357817	0.4232007	11.555583	13.035057

Measures	
-2*LogLikelihood	282.19237
AICc	286.55601
BIC	289.35941

Goodness-of-Fit Test

	W	Prob<W
Shapiro-Wilk	0.9184136	0.0113*

	A2	Simulated p-Value
Anderson-Darling	0.5925125	0.1080

(b) NASA TLX Shapiro-Wilk test result.

Figure 6.15: NASA TLX Test for normality results.

(Section 7.1.2) why we believed there was a slightly bigger range for the AI group in terms of workload.

Wilcoxon / Kruskal-Wallis Tests (Rank Sums)

Level	Count	Score Sum	Expected Score	Score Mean	(Mean-Mean0)/Std0
AI	18	352.500	333.000	19.5833	0.602
Non AI	18	313.500	333.000	17.4167	-0.602

2-Sample Test, Normal Approximation

S	Z	Prob>|Z|
313.5	-0.60160	0.5474

1-Way Test, ChiSquare Approximation

ChiSquare	DF	Prob>ChiSq
0.3812	1	0.5370

Figure 6.16: Workload Wilcoxon Rank Sums test results.

We provide a breakdown of the workload sub-scores in Table 6.3 and also provide a comparison between the two groups in Figure 6.18. The figure presents a line graph illustrating the breakdown of the six workload characteristic scores covered by the NASA TLX, which facilitates a clearer comparison between the two groups. The AI group shows higher mental, physical, and effort demands, but lower levels of temporal workload and frustration, along

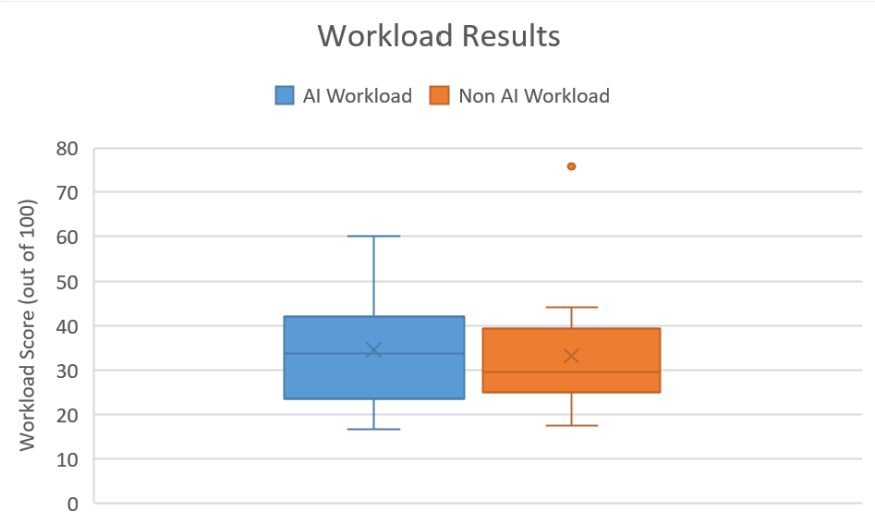


Figure 6.17: Workload box plot.

with better performance when compared to the non-AI group.

Table 6.3: Average NASA TLX Subscores based on Modalities.

Modality	Mental	Physical	Temporal	Performance	Effort	Frustration
AI Guided	40.83	19.72	11.67	84.44	37.78	13.67
Non AI Guided	37.94	18.61	14.00	83.06	32.5	13.72

6.3 Qualitative Results

Following the study, users were asked to answer some questions regarding their experience with the DT-learning platform. This allowed us to understand various areas that were successful and various areas that need to be worked on which will be discussed later in Chapter 7.

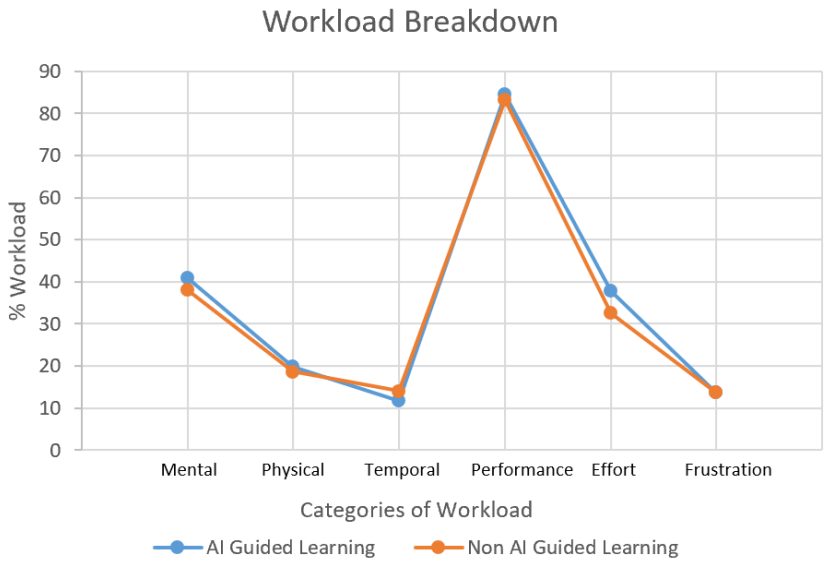


Figure 6.18: Workload comparison breakdown.

6.3.1 Features That Worked Well

Users were asked to share features that they believed worked well with the platform they experienced, and many highlighted the navigation mechanism as one of them. Participants expressed their appreciation for the teleportation system, highlighting its ease of use and suitability for new VR users. One participant noted:

> I liked the teleportation as it was very easy to use and learn as a new VR user.

While another remarked:

> The teleportation environment was good and is better than just continuous movement.

Users valued how the system allowed them to remain stationary, reducing physical effort, and praised the platform's ability to enhance focus by limiting navigation to relevant areas—an especially beneficial feature for those less familiar with VR.

Participants widely appreciated the integration of audio narrations with accompanying text, describing it as a highly effective feature. One participant remarked:

> The audio narration and the text mixed in together was really helpful so I can listen and also read off of something.

During the tutorial phase, audio narrations were supplemented with PowerPoint slides, while the practice phase combined audio narrations, text-based instructions, and user feedback to enrich the learning experience. Additionally, users praised the intuitive UI design and its responsiveness, particularly enjoying the interactive control panel that allowed them to manipulate water tanks and observe the changes both virtually and physically.

For the participants who were a part of the AI-guided learning group. The majority of users appreciated the use of an AI NPC character as it simulated the presence of a real teacher. They felt that this sense of presence helped them stay focused on the tasks and enhanced their learning experience.

6.3.2 Features that helped with Learning

Nearly all participants found the ”Learning by Doing” approach highly effective for mastering new concepts. They appreciated how the tutorial phase seamlessly combined traditional lectures with the opportunity to observe and experience cyberattacks firsthand. Users noted that learning through direct experience was more memorable than simply reviewing lecture slides, which enhanced information retention. One participant emphasized:

> While you were there and learning from the slides, you are able to interact with the system so you can think back to an experience instead of a lecture slide. This

> makes learning stronger since memory from the time when you were learning involved your senses.

The practice phase was also valued for reinforcing understanding, allowing users to test their knowledge, make mistakes, and refine their comprehension of cybersecurity concepts. Participants highlighted that the interactive elements made the learning process more engaging and enjoyable, which led to positive learning outcomes overall.

The DT concept was highly valued by most participants, as it enabled them to enhance their understanding by interacting with both the physical hardware and the virtual environment. One participant shared:

> Seeing how well things connected and the synchronization of the hardware and virtual environment felt more captivating.

Another user remarked:

> It was beneficial because it was useful to see the physical changes in real time. As a visual learner, it was helpful to see what is going on instead of just relying on the visual simulation, which is more practical for real-world scenarios.

Observing their actions reflected in both systems encouraged critical thinking and ensured that changes made in the VR environment were accurately captured by the webcam. The sound of the water pump turning on and off further reinforced this real-world connection, prompting users to pay closer attention and engage more deeply with the experience. When asked if the physical component was necessary, participants emphasized its importance, with many stating that the webcam was crucial for confirming whether the water level changed as expected. This added confidence in their decisions, as it allowed them to validate their observations.

6.3.3 Features needing improvement

Although users favored the teleportation mechanism overall, some users complained about certain characteristics of the teleportation mechanism. One of which was the color of the teleportation arch. Users had difficulty seeing it at times. Participants found the arch-based ray cast to be unnatural and difficult to use. They struggled to point at distant objects, as the mechanism felt disproportionate between their physical movements and the corresponding virtual actions.

While the majority of participants found the DT concept valuable, a few users did not share the same sentiment. One participant noted:

> It is an interesting concept, but I think it should be better integrated; however, the concept improved learning.

Another user remarked,

> It is hard to connect the virtual side with the physical side, and I thought having the virtual environment was enough.

These differing opinions highlight areas for improvement, which we will discuss later (Section 7.1.1).

Some of the users who participated in the Non-AI version of the practice phase found difficulty with the drop-down menu selection and did not like its design. Users were unable to select the answers at times. After further investigation, it was found that the drop-down menu required precise trigger button presses that novice VR users tended to struggle with.

AI-guided participants sometimes found the speech-to-text and text-to-speech systems to be inaccurate. Demonstrating that further refinement into this feature is needed. We discuss

more about specific observations in the next chapter.

Chapter 7

Discussion and Future Work

The results from the user study described in the previous chapter will help us analyze and answer our research questions which we do below. We also discuss general observations that were made during the conduction of the user study and point out areas that could be improved in future work.

7.1 Research Questions

In this section, we revisit the research questions and thoroughly analyze the results obtained from the study. By examining the data and insights gathered, we aim to provide clear and evidence-based answers to each research question, highlighting how the findings align with or deviate from initial expectations. This analysis not only addresses the core objectives of the research but also provides a foundation for interpreting the broader implications of the results.

7.1.1 RQ1: How does utilizing an XR-based DT platform for cybersecurity education influence participants' engagement, knowledge acquisition, and ability to interpret system behavior?

To answer this question, we had users interact with the DT concept by using the virtual environment as the UI for the hardware testbed and viewing changes on the hardware through the provided webcam footage. This allowed us to evaluate whether users appreciated interacting with the hardware and using it as a tool to observe cyberattacks and verify the outcomes of their actions.

Recalling hypothesis H1 (5.1), we stated that utilizing a VR platform for cybersecurity education would enhance participants' engagement, improve knowledge retention about cyberattacks, and support better interpretation of system behavior using information from the physical environment. As mentioned in Chapter 6, users were asked if they found the concept beneficial when learning about cyberattacks. Most of the users enjoyed the web camera view of the hardware as it allowed them to see the water level in the tank change to verify if their interaction with the control panel had the correct effect. This enabled them to use their observations to classify the cyberattacks properly. Hence, the results supported our hypothesis in this context.

On the other hand, a small portion of participants decided not to use the web camera view of the hardware and were able to accomplish the tasks, meaning there was a small population who found it unnecessary. With the scenarios that were programmed, it was possible for users to complete tasks without using the web camera to verify their actions on the hardware if they knew what to look for. Future work here would refine these scenarios further to encourage users to interact with the DT concept instead of relying solely on the

virtual side.

In summary, the majority of users relied on the web camera to observe changes in the system and found it necessary for learning the concepts. The DT concept was liked by many participants, demonstrating its potential. The number of users who found the web camera feature unnecessary was very small. Overall, incorporating both the virtual and physical components improved experiential learning outcomes and experiences in this use case.

One area for improvement in this regard was the quality of the web camera. Some users noted the web camera quality was poor due to blurriness. The webcams used consisted of 720p and 1080p cameras, which were easily viewed through a computer monitor. However, the poor quality may have been caused by integration issues with the Unity platform or hardware limitations of the VR headset. Future work would investigate the cause of the poor web camera quality to improve user experience and clarity.

7.1.2 RQ2: Does AI-guided learning have an impact on knowledge acquisition and experience when compared to non-AI guided learning?

As mentioned previously, we performed a between-subject design experiment that had an AI-guided learning group and a non-AI version. Our hypothesis (H2) for this research question from Section 5.1 was that AI Guided Learning would prove to have a better learning outcome and experience than the non-AI learning group.

The learning outcome was found to not have a significant difference between the AI-guided and non-AI-guided learning groups hence contradicting our hypothesis. However, we did see that the improvement score for the non-AI-guided group was better than the AI-guided

group. Two participants in the AI group did worse on the assessment after the study. This may have been caused by those participants not having an English background which made interacting with the AI difficult and may have confused them when they were learning the subject.

Another potential reason why the improvement score for the AI group was lower could be that users had to learn how to interact with the AI to receive the desired responses. Users were accustomed to interacting with humans through normal conversations; however, AI LLMs could not understand human conversations directly. To interact with LLMs effectively, prompt engineering may have needed to be considered. This is still a relatively new area of research, and researchers are investigating how to appropriately apply this technique in various contexts, such as academic writing and the medical field [15, 32], to achieve the desired responses efficiently. Future work could analyze how users could interact with AI LLMs effectively or investigate the concept of prompt engineering for educational purposes.

In terms of User Satisfaction (Section 6.2.3), calculations revealed no statistically significant difference in system usability and workload between the two groups. Looking at Table 6.2, the system usability score was lower for the AI group compared to the non-AI group. A potential reason for this might have been the inconsistency of the speech-to-text and text-to-speech functionality. During the study, some participants struggled with speaking to the AI character in English due to their comfort with the language. However, there were also instances where the speech-to-text functionality misunderstood fluent English speakers. Additionally, when the AI responded to users, random changes in tone and inappropriate pronunciations of words were observed, which might have affected users' experiences.

Although there were very few instances, the AI NPC character occasionally got lost in terms of navigation and context. The AI character became stuck in various locations of the virtual environment and failed to guide users to the correct location. Additionally, despite efforts

to refine the LLM and prevent issues, the AI NPC occasionally provided incorrect feedback to user responses, although such instances were less frequent. For example, when the correct answer was ”output data manipulation,” a user might have said ”input data manipulation,” and the AI incorrectly affirmed the user's response. This demonstrated that although AI was a valuable asset, it is still immature and inconsistent for heavy reliance.

The workload for the AI group was slightly higher than that of the non-AI group, likely due to the additional task of interacting with the AI character through conversation and eye contact. However, the difference was not statistically significant. Despite the slight increase in mental, physical, and effort demands, the AI-guided learning group demonstrated better performance, along with lower levels of temporal workload and frustration, compared to the non-AI-guided group. This suggested a potential trade-off.

Unlike the previous factors, presence was found to be statistically different for the AI-guided group compared to the non-AI group. Having the AI-guided character increased the users' sense of presence during the study. Participants noted that it felt as though an actual teacher was guiding them through the scenarios.

In summary, AI-guided learning did not significantly influence learning outcomes. However, it impacted many characteristics of the users' learning experiences, primarily their sense of presence. Presence was the only factor that showed a significant difference between the two groups. AI-guided learning enhanced the overall sense of presence. Although system usability and workload did not exhibit statistically significant differences, the study provided key insights and factors to consider in future work.

7.2 VR Environment

The VR environment successfully implemented the experiential learning concept. The tutorial phase fulfilled the requirements of the first two stages of Kolb's Learning Cycle (Concrete Experience and Reflective Observation), while the practice phase fulfilled the last two stages (Abstract Conceptualization and Active Experimentation). There was an improvement in knowledge across the board for all participants (Table 6.1). When participants shared their thoughts on the system, most expressed excitement about the platform and mentioned that it was more engaging than standard learning methods. Participants noted that while it was initially challenging to learn how to navigate the VR environment, they quickly became proficient with continued use and adapted to it effectively. It is important to note that the majority of participants had limited prior experience with VR before the study (Section 6.2.1), which presented a learning curve.

Future work for the VR environment would involve providing a more detailed integration with the hardware testbed. Currently, data from sensors and a webcam are used to display information from the hardware. However, user feedback indicated that while they appreciated the concept, the integration of the DT could have been improved. A detailed virtual miniature model of the hardware testbed within the virtual environment, with status details integrated into it, may prove to be more engaging and easier to understand and should be considered for future work.

7.3 Hardware Testbed

Our hardware was made up of Arduino components and various sensors. Although this hardware was affordable and cost-efficient, some of the hardware components were found

to be unstable during the study, which confused participants. More specifically, the water level sensor attached to the Arduino fluctuated randomly even though the water level was not changing. This was due to the water level sensor relying on electricity flowing through parallel wire tracks to determine the water level. Since the power supply only consisted of 5 volts, if other components or the NodeMCU were to change electricity usage, it would cause the water level sensor to provide different readings. This often confused users and we had to tell them to ignore it due to hardware tolerance. The pH level sensor also had low sensitivity, requiring significant changes in the solution's acidity or basicity to register a change. This prevented users from seeing the effect of the pH level change promptly. To summarize, because of these tolerances and reading issues with the sensors, participants were often confused by the sensor output and its fluctuations, especially with the water level sensor. If the product is to be commercialized or used in real-world scenarios, the hardware would need to be replaced with more stable and reliable hardware components while also maintaining affordability.

7.4 Using LLM for Cyberattacks

The original idea for this project was to have AI LLMs produce the cyberattack scripts for us instead of manually doing it ourselves. This proved to be very challenging due to the model's inconsistency in generating the right content continuously. In addition, many LLM models contain censorship and prevented us from generating appropriate attack commands since it is considered unethical and illegal depending on where the attack is performed. Attempts were made to manipulate the LLM to override its censorship such as telling it we were doing it for research purposes or that we were performing ethical hacking on a private network (prompt engineering) but those attempts failed.

We did consider the use of uncensored LLM models such as an offline Llama 2 model. However, these models needed to be hosted offline on computers. Due to this restriction, they tend to use smaller datasets which has proven the LLM to be inconsistent and unreliable. To make it usable, the model must be trained using a larger dataset. As a result, this would require significant computer processing power which increases costs. In summary, relying on AI LLMs for performing this type of task is not viable at the time of this writing due to its unstableness and immaturity. Future work would look into this area to determine a more viable solution.

7.5 Connecting Theory and Implementation

This section explains how the proposed system aligns with overall goals and Kolb's Learning Cycle, and how it contributed to achieving the research goals. We first talk about the first research goal which was investigating the potential of experiential learning through the developed system. To satisfy the four stages of Kolb's Experiential Learning Cycle, we implemented a two-phase structure within our VR environment. The **tutorial phase** introduced students to the concepts through interactive lessons, which fulfilled the first stage of Kolb's cycle, **Concrete Experience**. As part of these interactive lessons, we provided a functional, interactive water treatment control panel that allows users to observe a live demonstration of the water treatment plant's functionality before and after a cyberattack. This experience enabled users to understand the effects and outcomes of the attack, fulfilling the second stage of Kolb's cycle, **Reflective Observation**, by allowing them to observe the concepts in action.

The **practice phase** of the VR application addressed the latter half of Kolb's Learning Cycle, **Abstract Conceptualization** and **Active Experimentation**. In this phase, users were

presented with problem-solving tasks, enabling them to process ("think about") the concepts they have learned and apply them ("doing") to solve real-world challenges. This structure directly supported our research goal by providing a platform that integrated experiential learning techniques, allowing us to assess the effectiveness of this approach in enhancing user understanding of cybersecurity concepts.

The concept of a between-subjects design experiment allowed us to compare the learning and experience outcomes of our system when users interacted with an AI-guided NPC versus when they did not. That is why our practice phase contained two different modalities. This design helped us address the second research goal of evaluating the effectiveness of human-like interactions with AI-driven NPCs in education.

In our system, we integrated both virtual and physical components to provide a more comprehensive and intuitive understanding of cybersecurity attacks. The virtual component, which we presented through VR, simulated the operational aspects of a water treatment plant that the physical system could not, offering users a visual and interactive representation of the plant's systems. This virtual representation allowed users to engage with and manipulate the system, observing how the cyberattack impacted the processes in real-time and see the effects.

On the other hand, the hardware components consisted of a physical testbed, which mimicked the real-world infrastructure of the water treatment plant in a more cost-efficient manner and provided the IoT infrastructure needed to conduct and demonstrate the cyberattacks. This hardware testbed was connected to the VR environment, allowing for the integration of real-world devices such as sensors and control panels. The physical testbed enabled the observation of the direct effects of cyberattacks on the devices, making the attack's input (e.g., system manipulation) and output (e.g., data corruption) clearer and more perceptible.

Chapter 8

Conclusions

Traditional learning methods have been shown to be less effective compared to experiential learning. Additionally, the growing adoption of DT applications is driving industry demand, yet the next generation of students remains largely unfamiliar with this concept. In collaboration with a workforce development program between Virginia Tech and Virginia Military Institute, we presented a new immersive and interactive learning platform designed to enhance learning outcomes by fostering user engagement and providing experiences that promote concept retention.

We started by introducing the concept of DT and the motivation for our work. Followed by a literature review of the current research involving the DT concept and VR experiential learning platforms. Through this, we discovered that the concept of DT being used with VR in parallel is not very common. We then proposed an experiential learning platform that integrated the concepts of DT and VR to provide a better learning experience.

The potential of this platform was demonstrated through a case study that educated cybersecurity concepts in the context of water treatment plant facilities. A between-subject study design was conducted with two different groups: AI-guided learning and non-AI-guided learning. Results showed that presence was increased with the use of AI-guided learning and that workload and system usability scores were statistically the same between the two groups. Although there was no significant difference in learning improvement between the two groups, the increase in assessment scores, which was found to be statistically different,

across all participants demonstrated that this type of platform had the potential to be an effective learning tool. User reviews demonstrated its effectiveness in terms of user engagement compared to traditional learning methods, along with providing insights into areas that could be further improved.

In conclusion, this type of platform has proven to be a great step towards the shift from traditional learning methods to experiential learning methods. Our platform has demonstrated its ability to improve overall learning experiences. AI has shown to not negatively affect experiences but actually improved the users sense of presence and engagement through experiences. Despite the platform performing well for the first of its kind, we have seen that improvements need to be made in order to adopt this in real world applications and some adaptations of the concepts were not suited for all. We hope that this work motivates the change from traditional lecture-style learning to a more engaging and interactive learning experience. The concept has been demonstrated to be effective through our case study but further improvements need to be made if this concept is to be commercialized for practical use.

Bibliography

[1] B Danette Allen. Digital Twins and Living Models at NASA - NASA Technical Reports Server (NTRS), Nov 2021. URL https://ntrs.nasa.gov/citations/20210023699. Last accessed 11 December 2024.

[2] Abdullah Alnajim, Shabana Habib, Muhammad Islam, Hazim AlRawashdeh, and Muhammad Wasim. Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*, 15:2175, 12 2023. doi: 10.3390/sym15122175.

[3] Natalie Neysa Alund. Honda Recalls More Than 750,000 Vehicles for Airbag Issue: Here's What Models are Affected, Feb 2024. URL https://www.usatoday.com/story/money/cars/recalls/2024/02/06/honda-recall-accord-civic-pilot-crv-airbag-issue/72489945007/. Last accessed 11 December 2024.

[4] Janjira Aphirakmethawong, Erfu Yang, and Jörn Mehnen. An Overview of Artificial Intelligence in Product Design for Smart Manufacturing. In *2022 27th International Conference on Automation and Computing (ICAC)*, pages 1–6, 2022. doi: 10.1109/ICAC55051.2022.9911089.

[5] Matthew L. Bolton, Elliot Biltekoff, and Laura Humphrey. The Mathematical Meaninglessness of the NASA Task Load index: A level of Measurement Analysis. *IEEE Transactions on Human-Machine Systems*, 53(3):590–599, 2023. doi: 10.1109/THMS.2023.3263482.

[6] Nathan Bomey. How Chinese Military Hackers Allegedly Pulled off

the Equifax Data Breach, Stealing Data from 145 Million Americans, Feb 2020. URL https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/. Last accessed 11 December 2024.

[7] Dylan Butts. FAA audit of Boeing's 737 MAX Production Reportedly Found "Dozens of Issues", Mar 2024. URL https://www.cnbc.com/2024/03/12/faa-audit-of-boeings-737-max-production-found-dozens-of-issues-nyt.html. Last accessed 11 December 2024.

[8] Mario Catalano, Alessandro Chiurco, Caterina Fusto, Lucia Gazzaneo, Francesco Longo, Giovanni Mirabelli, Letizia Nicoletti, Vittorio Solina, and Simone Talarico. A Digital Twin-Driven and Conceptual Framework for Enabling Extended Reality Applications: A Case Study of a Brake Discs Manufacturer. *Procedia Computer Science*, 200:1885–1893, 2022. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2022.01.389. 3rd International Conference on Industry 4.0 and Smart Manufacturing.

[9] The AnyLogic Company. Anylogic, 2000. URL https://www.anylogic.com/. Last accessed 11 December 2024.

[10] Wikipedia contributors. The four steps in Kolb cycle. https://en.wikipedia.org/wiki/File:The_Four_Steps_in_Kolb_Cycle.svg, 2024. Last accessed 11 December 2024.

[11] Trace William Cowen. Easy NYC Turnstile Hack Emerges Amid Rollout of $700,000 Pilot Program Aimed at Fare Evasion. Complex, Jan 2024. URL https://www.complex.com/life/a/tracewilliamcowen/nyc-turnstile-hack-video. Last accessed 11 December 2024.

[12] Th DiNapoli. Annual Update: Metropolitan Transportation Authority's Debt Profile, 2022. URL https://www.osc.ny.gov/files/reports/osdc/pdf/mta-debt-rpt-1-2022.pdf. Last accessed 11 December 2024.

[13] Nikitha Donekal Chandrashekar, Anthony Lee, Mohamed Azab, and Denis Gracanin. Understanding User Behavior for Enhancing Cybersecurity Training with I]mmersive Gamified Platforms. *Information*, 15(12), 2024. ISSN 2078-2489. doi: 10.3390/info15120814.

[14] Jen Easterly and Tom Fanning. The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years: CISA. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years, May 2023. Last accessed 11 December 2024.

[15] Louie Giray. Prompt Engineering with ChatGPT: A Guide for Academic Writers. *Ann. Biomed. Eng.*, 51(12):2629–2633, December 2023. doi: 10.1007/s10439-023-03272-4.

[16] Irene Gironacci. XR Management Training Simulator Supported by Content-Based Scenario Recommendation. In *2022 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, pages 104–108, 2022. doi: 10.1109/AIVR56993.2022.00021.

[17] Edward H Glaessgen. The Digital Twin Paradigm for future NASA and U.S. Air Force Vehicles - NASA Technical Reports Server (NTRS), Apr 2012. URL https://ntrs.nasa.gov/citations/20120008178. Last accessed 11 December 2024.

[18] Michael Grieves. Digital twin: Manufacturing Excellence Through Virtual Factory Replication. *White paper*, 1(2014):1–7, 2014.

[19] Jordan Henstrom, Raffaele De Amicis, Christopher A Sanchez, and Yelda Turkan. Immersive Learning in Engineering: A Comparative Study of VR and Traditional Building Inspection Methods. In *Proceedings of the 28th International ACM Conference on 3D Web Technology*, Web3D '23, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9798400703249. doi: 10.1145/3611314.3615917.

[20] Weifei Hu, Tongzhou Zhang, Xiaoyu Deng, Zhenyu Liu, and Jianrong Tan. Digital Twin: A state-of-the-art Review of its Enabling Technologies, Applications and Challenges. *Journal of Intelligent Manufacturing and Special Equipment*, 2(1):1–34, Jul 2021. doi: 10.1108/jimse-12-2020-010.

[21] Convai Technologies Inc. Embodied ai characters for virtual worlds. https://convai.com/, October 2024. Last accessed 11 December 2024.

[22] Zhou Jin and Zhou Meiyu. Research on the Effectiveness of Experiential Learning in Immersive Virtual Reality. In *2020 International Conference on Modern Education and Information Management (ICMEIM)*, pages 828–831, 2020. doi: 10.1109/ICMEIM51375.2020.00184.

[23] David Kolb. *Experiential Learning: Experience As The Source Of Learning And Development*, volume 1. Prentice Hall, 01 1984. ISBN 0132952610.

[24] Andreas Komninos and Georgios Tsigkas. Prototyping a Digital Twin System for Environmental Education. In *Proceedings of the 26th Pan-Hellenic Conference on Informatics*, PCI '22, page 361–366, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9781450398541. doi: 10.1145/3575879.3576018.

[25] Heiner Lasi, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. Industry 4.0. *Business & Information Systems Engineering*, 6(4):239–242, 2014. ISSN 1867-0202. doi: 10.1007/s12599-014-0334-4.

[26] Paula Lauren and Paul Watta. Work-in-progress: Integrating Generative AI with Evidence-based Learning Strategies in Computer Science and Engineering Education. In *2023 IEEE Frontiers in Education Conference (FIE)*, pages 1–5, 2023. doi: 10.1109/FIE58773.2023.10342970.

[27] Anthony Lee, Kenneth King, Denis Gračanin, and Mohamed Azab. Experiential Learning Through Immersive XR: Cybersecurity Education for Critical Infrastructures. In Abbas Moallem, editor, *HCI for Cybersecurity, Privacy and Trust*, pages 56–69, Cham, 2024. Springer Nature Switzerland. ISBN 978-3-031-61382-1. doi: 10.1007/978-3-031-61382-1_4.

[28] James R. Lewis. The System Usability Scale: Past, Present, and Future. *International Journal of Human–Computer Interaction*, 34(7):577–590, 2018. doi: 10.1080/10447318.2018.1455307.

[29] Sean Lyngaas. Russia-linked Hacking Group Suspected of Carrying Out Cyberattack on Texas Water Facility, Cybersecurity Firm Says | CNN politics, Apr 2024. URL https://www.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack/index.html. Last accessed 11 December 2024.

[30] Katerina Mangaroska and Michail Giannakos. Learning Analytics for Learning Design: A systematic Literature Review of Analytics-Driven design to Enhance Learning. *IEEE Transactions on Learning Technologies*, 12(4):516–534, 2019. doi: 10.1109/TLT.2018.2868673.

[31] Saul McLeod. Kolb's Learning styles & Experiential Learning Cycle, Feb 2024. URL https://www.simplypsychology.org/learning-kolb.html. Last accessed 11 December 2024.

[32] B. Meskó. Prompt Engineering as an Important Emerging Skill for Medical Professionals: Tutorial. *J Med Internet Res*, 25(e50638), 2023. doi: 10.2196/50638.

[33] Carlos Miskinis. The Mysterious History of Digital Twin Technology and Who Created it, Mar 2019. URL https://www.challenge.org/insights/digital-twin-history/. Last accessed 11 December 2024.

[34] Tatsuya Ono and Tomokazu Ishikawa. A Research on Penalty Kick Training System Using XR. In *2023 Nicograph International (NicoInt)*, pages 86–86, 2023. doi: 10.1109/NICOINT59725.2023.00026.

[35] Donatella Persico and Francesca Pozzi. Informing Learning Design with Learning Analytics to Improve Teacher Inquiry. *British Journal of Educational Technology*, 46(2): 230–248, 2015. doi: https://doi.org/10.1111/bjet.12207.

[36] Vipula Rawte, Swagata Chakraborty, Agnibh Pathak, Anubhav Sarkar, S.M Towhidul Islam Tonmoy, Aman Chadha, Amit Sheth, and Amitava Das. The troubling emergence of hallucination in large language models - an extensive definition, quantification, and prescriptive remediations. In Houda Bouamor, Juan Pino, and Kalika Bali, editors, *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, pages 2541–2573, Singapore, December 2023. Association for Computational Linguistics. doi: 10.18653/v1/2023.emnlp-main.155.

[37] Fatemeh Sarshartehrani, Anthony Lee, Mohamed Azab, Trenton Watkins, and Denis Gračanin. Towards Immersive Cybersecurity Workforce Development for Mission-Critical Iot Systems. In *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0176–0182, 2024. doi: 10.1109/UEMCON62879.2024.10754707.

[38] Thomas Schubert, Frank Friedmann, and Holger Regenbrecht. The Experience of Presence: Factor Analytic Insights. *Presence: Teleoperators and Virtual Environments*, 10 (3):266–281, 06 2001. doi: 10.1162/105474601300343603.

[39] Kshitij Sharma, Hamed S. Alavi, Patrick Jermann, and Pierre Dillenbourg. A Gaze-based Learning Analytics Model: In-video Visual Feedback to Improve Learner's Attention in MOOCs. In *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge*, LAK '16, page 417–421, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450341905. doi: 10.1145/2883851.2883902.

[40] Yoana Slavova and Mu Mu. A Comparative Study of the Learning Outcomes and Experience of VR in Education. In *2018 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 685–686, 2018. doi: 10.1109/VR.2018.8446486.

[41] Ron Snijders, Paolo Pileggi, Jeroen Broekhuijsen, Jacques Verriet, Marco Wiering, and Koen Kok. Machine Learning for Digital Twins to Predict Responsiveness of Cyber-Physical Energy Systems. In *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, pages 1–6, 2020. doi: 10.1109/MSCPES49613.2020.9133695.

[42] Qiao Sui and Li Sui. Research on the Impact of Interactive Experience and Perceived Value on User Satisfaction in VR Education. In *2024 13th International Conference on Educational and Information Technology (ICEIT)*, pages 206–211, 2024. doi: 10.1109/ICEIT61397.2024.10540855.

[43] Fei Tao, Jiangfeng Cheng, Qinglin Qi, Meng Zhang, He Zhang, and Fangyuan Sui. Digital Twin-driven Product Design, Manufacturing and Service with Big Data. *The International Journal of Advanced Manufacturing Technology*, 94(9):3563–3576, 2018. ISSN 1433-3015. doi: 10.1007/s00170-017-0233-1.

[44] New York City Transit. MTA Installs Platform Barriers at 191st St 1 Station, Jan 2024. URL https://new.mta.info/press-release/mta-installs-platform-barriers-191-st-1-station. Last accessed 11 December 2024.

[45] Yuying Wei, Adrian Wing-Keung Law, and Chun Yang. Real-Time Data-Processing Framework with Model Updating for Digital Twins of Water Treatment Facilities. *Water*, 14(22), 2022. ISSN 2073-4441. doi: 10.3390/w14223591.

[46] Gary White, Anna Zink, Lara Codecá, and Siobhán Clarke. A Digital Twin Smart City for Citizen Feedback. *Cities*, 110:103064, 2021. ISSN 0264-2751. doi: https://doi.org/10.1016/j.cities.2020.103064.

[47] Korah J. Wiley, Yannis Dimitriadis, Allison Bradford, and Marica C. Linn. From Theory to Action: Developing and Evaluating Learning Analytics for Learning Design. In *Proceedings of the Tenth International Conference on Learning Analytics & Knowledge*, LAK '20, page 569–578, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450377126. doi: 10.1145/3375462.3375540.

[48] Jun Xiao, Xuejiao Li, and Lamei Wang. Applying Learning Analytics to Assess Learning Effect by Using Mobile Learning Support System in U-Learning Environment. In *2019 10th International Conference on Information Technology in Medicine and Education (ITME)*, pages 294–298, 2019. doi: 10.1109/ITME.2019.00074.

[49] Qinghua Xu, Shaukat Ali, and Tao Yue. Digital Twin-based Anomaly Detection in Cyber-physical Systems. In *2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST)*, pages 205–216, 2021. doi: 10.1109/ICST49551.2021.00031.

[50] Xun Xu, Yuqian Lu, Birgit Vogel-Heuser, and Lihui Wang. Industry 4.0 and Industry

5.0—inception, Conception and Perception. *Journal of Manufacturing Systems*, 61: 530–535, Oct 2021. doi: 10.1016/j.jmsy.2021.10.006.

[51] Shuhei Yoshida, Toru Abe, and Takuo Suganuma. Design of a Support System for Guitar Performance Training Using XR Technology. In *2023 IEEE 12th Global Conference on Consumer Electronics (GCCE)*, pages 276–279, 2023. doi: 10.1109/GCCE59613.2023.10315398.

[52] Yuhang Zhao, Shanchen Pang, Zhihan Lv, and Sheng Miao. Augmented Digital Twins for Predictive Automatic Regulation and Fault Alarm in Sewage Plan. In *Proceedings of the 31st ACM International Conference on Multimedia*, MM '23, page 8495–8503, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9798400701085. doi: 10.1145/3581783.3613778.

[53] Zhaofeng Zhong, Chamith Wijenayake, and Chamira U. S. Edussooriya. Exploring the Performance of Generative AI Tools in Electrical Engineering Education. In *2023 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, pages 1–6, 2023. doi: 10.1109/TALE56641.2023.10398370.

[54] Lexin Zhou, Wout Schellaert, Fernando Martínez-Plumed, Yael Moros-Daval, Cèsar Ferri, and José Hernández-Orallo. Larger and more instructable language models become less reliable. *Nature*, 634(8032):61–68, October 2024. ISSN 1476-4687. doi: 10.1038/s41586-024-07930-y.