Experiential Learning Through Immersive XR: Cybersecurity Education for Critical Infrastructures

Anthony Lee[1(✉)], Kenneth King[1], Denis Gračanin[1], and Mohamed Azab[2]

[1] Virginia Tech, Blacksburg, VA 24060, USA
{leean1,kking93,gracanin}@vt.edu
[2] Virginia Military Institute, Lexington, VA 24450, USA
azabmm@vmi.edu

Abstract. In our modern digital world, where virtually everything is intertwined with computer systems, critical infrastructures face vulnerability to a variety of cyber-attacks, stemming from the absence of a cybersecurity mindset within these establishments. We need to efficiently educate these workers about the cybersecurity threats that exist, their potential effects, and the subsequent substantial impact on human populations. Previous research has suggested traditional non-interactive training methods are often not effective. We propose an interactive learning experience that incorporates Extended Reality, Digital Twins, and Artificial Intelligence (AI) to help workers become more aware of cybersecurity issues within their critical infrastructure. This paper introduces an innovative testbed that seamlessly integrates Artificial Intelligence (AI) and Large Language Models to create an immersive educational experience. The goal is to effectively convey complex technical concepts to users with limited background knowledge on the subject. Our specific focus lies in addressing the need for proper cybersecurity training among water treatment plant employees.

The testbed presented is meticulously crafted to provide users with a tangible representation of the potential outcomes resulting from successful cyber attacks on such facilities. Through this approach, we aim to enhance the educational process and promote a deeper understanding of cybersecurity challenges in critical infrastructure like water treatment plants.

Keywords: Artificial Intelligence (AI) · Digital Twins · Critical Infrastructures · Cybersecurity · Large Language Models (LLM) · Internet of Things (IoT)

1 Introduction

Cyberattacks are a pressing matter in today's digital world but people do not take the necessary initiative to prevent them. A relevant example can be seen

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 56–69, 2024.
https://doi.org/10.1007/978-3-031-61382-1_4

from the Colonial Pipeline Cyber-attack that happened on May 7, 2021, where a major pipeline supplying gas throughout the East Coast was hit with a ransomware attack [6]. The attack was caused by an exposed password that provided access to the pipeline's network. Another example was the Equifax data breach that happened back in 2017 which resulted in 145 million people's personal information being leaked. The breach could have easily been prevented if Equifax had installed security updates [2]. Both of these events could have been easily prevented if people didn't neglect the importance of cybersecurity. Such events contributed to a wake-up call to the United States for its aging critical infrastructure and lack of cybersecurity awareness.

We have seen that humans are frequently the most vulnerable element in any cyber system. Many sophisticated attacks leverage human errors, vulnerabilities, or evident flaws throughout different phases. Even with substantial research dedicated to understanding and rectifying human mistakes in cyber-attack and defense contexts, there is a broad agreement that no single model entirely addresses this aspect or corrects it with optimal efficacy. These variables can change based on the individual involved, the specific environment, and the nature of the threat or defense situation. In scenarios involving mission-critical applications, the risk, and associated mitigation costs escalate significantly.

This paper seeks to bridge the gap in interactive and IoT-based system simulators for cybersecurity training. Research indicates that an interactive and immersive training approach, incorporating the principles of IoT technology, significantly enhances learning outcomes [9]. We introduce an affordable, programmable, fully immersive testbed that utilizes the digital twin concept to produce a realistic representation of a mission-critical infrastructure, a wastewater treatment plant. This testbed is designed to enhance the training and education of cybersecurity concepts. It achieves this by immersing users in an operational context where the system is under attack. There are various scenarios where attacks are based on user errors or by exploiting cyber vulnerabilities that can be better exposed with cybersecurity-unaware human interaction. Leveraging Large Language Models (LLMs), the testbed creates motivational strategies that provoke such human errors, paving the way for further attack avenues. In addition, LLMs allow non-experts in cybersecurity to translate high-level requests into low-level attack scenarios conducted on the testbed. The result is then portrayed in Extended Reality (XR) to intensify user immersion and generate an authentic representation of real-world attack situations.

Section 2 reviews the previous work that has been completed and what this paper aims to continue. Section 3 describes the problem and related challenges and why it is important to address them. Section 4 provides an overview of the proposed system and how all of the components interact with each other. The methodology used is described in Sect. 5 and the findings are provided in Sect. 6. Section 7 concludes the paper and provides directions for future work.

2 Literature Review

2.1 XR-Enabled Immersive Training Experiences

Introducing interactive components such as XR can allow for greater concentration and enhanced learning. Gironacci [8] proposes a training simulator where XR and AI are infused together to provide dynamic feedback based on a user's input and interaction. The simulator uses Natural Language Processing (NLP) to identify keywords and then make suggestions that are aimed to help them learn why a particular action should be taken. Yoshida et al. [17] presents an XR-based guitar training system that aims to expand previous research by using XR technology to provide performance skill training: teaching users how much force to apply and providing timing feedback. However, Artificial Intelligence (AI) was not used to provide real-time feedback to help the trainee correct behavior to play better. One of the suggested improvements from the case study was having markers on the actual guitar so each user would know where to place their fingers when playing. This would depend on the specific song being played so it would be impractical for the markers to be manually configured for each song. Instead, we could use AI and train the model with a guitar-playing dataset so that markers could be placed dynamically based on the song they selected. A soccer XR training simulator [14] also uses XR to train players in performing goal kicks using a series of image recognition software and a camera. AI could be integrated into this use case for analyzing the parameters and providing suggestions on how to improve the kick autonomously.

Another similar XR-based simulator was also created for training within the medical field [4]. More specifically, an immersive training environment was created for Pulse Palpating Training. The simulator provides haptic, visual, and auditory feedback and aims to provide realism in a stress-free environment when training the next generation of medical professionals. Most equipment options currently available are expensive and do not even provide a full set of simulation capabilities.

Conducting cybersecurity training directly on an expensive piece of equipment is not feasible, especially given possible environmental and other impacts. This paper introduces an ergonomic and cost-effective method for enhancing realism in cybersecurity training, enabling operators to thoroughly understand and engage with the concepts so that preventative measures can be taken to prevent drastic failures.

2.2 Cybersecurity Training and Education Challenges

Cybersecurity is increasingly problematic due to cyberattacks on sensitive platforms, so it's crucial to address these issues promptly to prevent further escalation. We focus on water treatment plants as many critical issues need to be addressed. For instance, one problem is that the water treatment plants are not kept up to date as they use legacy systems and outdated technologies. Operators don't tend to think about how outdated their system is and just think about

whether the system functions correctly and only make changes if necessary. This is the wrong mindset in today's digital age as cyberattacks occur much more commonly than in the past. Legacy systems also tend to have short-term data retention which is unacceptable as we derive statistical models using large data sets to help make improvements in terms of automation. This in turn helps identify vulnerabilities and optimizations to create a more sophisticated and secure system [11].

Another need for cybersecurity training within critical infrastructures is due to their large impact on the surrounding population. We have already seen how an attack on a fuel pipeline has impacted the United States as it caused panic, shortages, and inflated gas prices [6]. This is due to the lack of cybersecurity training and awareness among the workers which causes operators to be vulnerable to social engineering and phishing attacks that allow attackers to gain access to the system using their credentials [15]. These issues motivate the development of an interactive cybersecurity training system to promote cybersecurity thinking within the workplace.

2.3 Innovations in Cybersecurity Training Platforms

The initial efforts that provide the foundation of the work are described in [3] where an XR-based IoT simulator (testbed) for a water treatment plant is proposed so that Cyber-Physical Systems can be integrated into cybersecurity education. The development of a water treatment digital twin was informed by first analyzing the weaknesses of the current water treatment plants discussed in Sect. 2.2. By having the testbed, an interactive and immersive education experience will inform operators of how serious these issues are and why it is important that they don't be ignored. The experiential learning experience will help operators visualize the consequences of certain actions and explore the system's vulnerabilities. In addition, its capabilities can be expanded beyond education and be used for simulation purposes (pen testing) to ensure the best cybersecurity posture.

In this paper, we use AI to create attack and defense scenarios, converting complex requests into understandable cyberattack situations. This approach facilitates the translation of low-level cyber-attacks for a broader audience, aiding non-experts in grasping necessary safety measures. Moreover, it assists plant operators in identifying overlooked vulnerabilities and offers real-time feedback for enhancing defense mechanisms.

Nagarajan et al. [13] proposed that video games should be used for cybersecurity training to attract more attention to important cybersecurity training topics. The use of LLMs can help generate dynamic content within the video game that allows users to remain attracted. For example, when a user creates their user profile in a video game, AI can use that information to dynamically form a phishing or social engineering attack unique to the user. This will allow the players to experience the manipulation that goes behind these attacks so that they learn not everyone can be trusted. XR can further enhance the immersive interaction experience.

3 The Proposed Use-Case: An XR-Enabled Waste Water Treatment Educational Testbed

Critical infrastructures are essential to our way of life, providing the necessary resources for our daily activities. Examples of critical infrastructures include power plants, water treatment plants, and communication networks. A failure in any of these systems would have devastating consequences for our society. For example in water treatment plants, a failure would adversely affect the surrounding environment, leading to environmental pollution and significant disruption in agricultural activities.

Water Treatment Plants are responsible for processing and purifying our wastewater before it is released back into the environment, emphasizing that each step of the water treatment process is critical. Failures caused by cybersecurity breaches can easily be avoided with the right mindset and the proper training. Most cybersecurity training courses today aren't engaging due to their lack of immersiveness and adaptability to various scenarios [9]. Using LLMs enables trainees to engage with a Conversational AI agent for translating high-level concepts into low-level ones, enhancing their grasp of cybersecurity and its impact. The XR component allows us to illustrate attack effects in a Virtual Environment, creating a more immersive training experience.

This paper uses LLMs to focus on educating trainees about Denial of Service Attacks. Our primary objective is to propose a strategy to diminish the vulnerability to these threats. We specifically concentrate on the prevalent issue of insufficient training and education among staff and operators at water treatment facilities. We contend that our proposed solution, a comprehensive and interactive cybersecurity training system, will significantly enhance awareness and understanding of cybersecurity threats among all stakeholders. By doing so, we aim to ensure the rigorous implementation of appropriate measures and protocols to safeguard against these ever-evolving digital dangers.

4 System Overview

The proposed system (Fig. 1) provides an immersive experience for trainees by having them placed into an *XR Environment* where they can interact with a *Conversational AI Agent*. *Conversational AI Agent* interacts with the users in *XR Environment* to understand what type of attack objectives the user would like to achieve. In addition to that, the agent can answer any lingering questions so that the user will be able to fully learn the concepts that will help them perform their jobs better. Once an attack objective has been decided, it sends the attack objectives and targets to the *Physical AI Agent* who is then responsible for performing the attack on the *Physical Environment* (the testbed). This is done by using an attack script in combination with LLMs as described in Sect. 5.1 where the script will execute attacks through the command line interface of the*Physical Environment*.

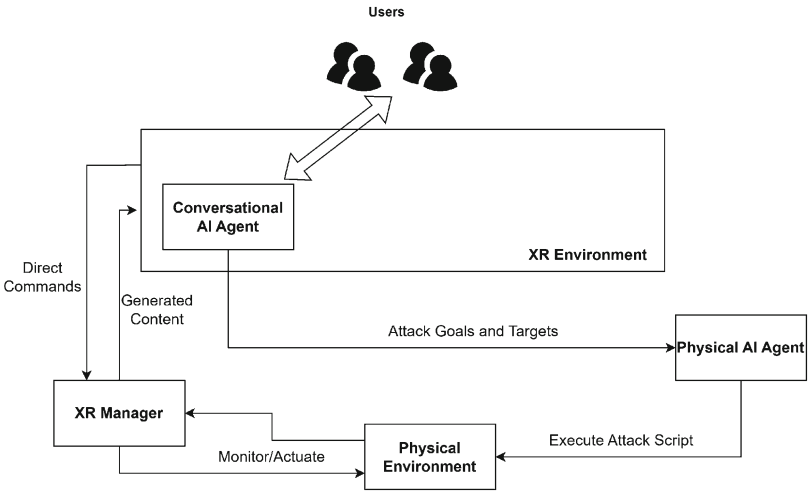

Fig. 1. The testbed architecture.

The *Physical Environment* and *XR Manager* exchange data using the MQTT protocol so that the *XR Manager* can generate the effect of the changes made to the *Physical Environment* back to the *XR Environment* where the users can witness the changes in real-time. This approach enables trainees to experience the impact of cyberattacks as if they were physically present and to engage with control modules to address the problem. Through such simulations, where users actively attempt to manage or mitigate unfolding issues or are subject to deception, they can gain a comprehensive understanding of the critical importance of cybersecurity in their field and learn effective response strategies for real-world scenarios.

Fig. 2. The testbed hardware implementation.

The testbed [3] setup (Fig. 2) replicates the water treatment process in a controlled, smaller-scale environment to ensure safety and affordability. The first stage in the water treatment plant is the water intake process where the sewer water is brought into the facility. During this step, various sensors measure the water intake rate and monitor the water levels to ensure efficient intake. If the system sensors were to be manipulated, this could cause either an overflow or underflow of water into the treatment plant which would then have other catastrophic impacts such as the sewer system being backed up or water contamination due to flooding.

The water is then cleansed of any garbage that may be in the sewage using a mesh netting system. After this step, the water is purified by removing liquid pollutants like kitchen grease through an extensive skimming system. This system features a large mechanical arm designed to skim oils off the water's surface while it resides in a large pool.

Additionally, the system includes monitoring controls that regulate the skimming arm's speed and manage the flow rate of the water in the pool, ensuring efficient and thorough removal of contaminants. This system could be exploited as having the water flow too fast or having the arm move at an improper speed would prevent the chemicals from being skimmed off.

The wastewater then goes through another filtration process that removes any biological organisms which involves adding various chemicals and monitoring the temperature and pH levels. To ensure the proper modifications, various sensors measure each of these parameters. Once this process is finished, the water goes through a chlorination process so that the water can be made usable which also involves the use of a sensor to monitor chlorine levels. If any of these sensors fail during the treatment process, it may render the water unusable, leading to biological harm and adverse health effects.

5 The Main System Actors

We use XR and LLM-driven attack and defense scenarios to fully demonstrate the impact of cyber security attacks on mission-critical systems dynamically and adaptively. The proposed testbed involves the use of two AI Agents: *Physical AI Agent*, and *Conversational AI Agent.*

5.1 Physical AI Agent

Physical AI agent uses LLMs to play the role of an attacker performing autonomous vulnerability analysis against the IoT systems in a water treatment testbed. To perform this autonomous vulnerability analysis, we use a popular network scanner Nmap [12] that scans the various active networks on the testbed and provides a list of open ports and corresponding services that are executing on that port. These vulnerability scanning results will then be processed by the LLM to determine the most appropriate target to perform the Denial of Service attack on.

For the LLM task of Nmap analysis, we found that the current leading open-source models (namely Llama2 at the time) performed so poorly that they could not be used reliably. In contrast, the leading closed-source model at the time, OpenAI's GPT-4 [16], was able to identify ports and IP addresses of interest with strong accuracy. While we would have preferred to use entirely open-source models, we were forced to use GPT-4 (gpt-4-0613 specifically) given no open-source LLM could perform the tasks desired reliably in comparison.

For the LLM task of generating attack commands for the Hping tool [1], we found that both GPT-4 and Meta's Llama2 would often refuse the task, given their built-in alignments and safety features. Therefore, we employed an uncensored version of Llama2 from TheBloke called Luna-AI-Llama2-Uncensored [10]. Compared to other uncensored LLMs on Hugging Face, we found that this model provided the same level of accuracy with faster response times. Similar to the Nmap analysis task, this open-source model struggled to consistently generate properly formatted attack commands. At the same time we found that although GPT-4 refused to generate attack commands, it would happily fix any errors in attack commands generated by another model. Therefore, we implemented a filtering mechanism so that after the uncensored model generates the attack command, GPT-4 corrects any errors in the command before returning the final result.

To bridge the gap between the high-level attack objectives and low-level cyberattacks, we use the LangChain framework which helps us integrate LLMs into our application to make more accurate decisions by using the Output Parser functionality [5]. LangChain allows us to provide LLMs with specific prompts and context when generating responses so they can make informative decisions. LangChain guides the LLM in classifying the attack, translating the information from a novice-friendly level to something comprehensible for an expert.

Scenario Generation Example: Let's say an attacker wanted to stop the facility from functioning properly. The AI, with the help of LangChain [5], would interpret that a Denial of Service Attack is desired. The AI-driven attack agent would use the Nmap tool [12] to identify which IP addresses and ports are currently running on the testbed. The attack agent will process the information, identify the services running on each host, and learn of their known vulnerabilities to determine which host and port would be feasible to perform a flooding attack. The outcome of such a step will be the seed for the attack scenario generation. The agent will then generate attack commands using the Hping tool, which will successfully exploit such vulnerabilities in a multi-stage process.

5.2 Conversational AI Agent

As part of our platform, we want the player to be able to interact with a cybersecurity expert within the XR environment who will be able to help guide players through learning the concepts. We introduce an NPC character that provides Natural Language conversations and human-like interactions. A 3D humanoid

model is created within the Unity Engine along with a waypoint-based navigation system programmed through C# that provides it with basic movement automation. It also can interact with players like in normal human-to-human interaction as the NPC can turn to face players wherever they are. To facilitate natural language conversations, we use OpenAI's ChatGPT-4 Model where players are essentially connected with a live expert.

During development, we faced challenges in maintaining real-time responses with the AI as player interactions did not synchronize with the NPC's actions that were portrayed within the XR environment. This was caused by our attempt to add Meta Quest input capabilities for interacting with the NPC. The Unity assets we used were originally designed to be used within the Unity environment and not through a VR headset, therefore limitations were presented with attempting to get the Meta Quest VR headset to interact with the NPC.

5.3 The XR Environment

Based on the work presented in [3] we created an XR environment that provides a real-life interactable digital twin version of the testbed using the Unity Engine [7]. The environment consists of many different objects within the Unity Engine, including prefabs that represent real-life components of the water treatment plant. By having these objects, we can place buttons that allow simulation capabilities of the different components of the Water Treatment Plant. Each button has been attached to a method that then calls a script to interact with the physical testbed providing the connection from the virtual world to the physical world and helping trainees visualize their actions. An MQTT Broker method is used for communication between the virtual environment and the testbed. We then assign call methods for each functionality of the water treatment process and assign them so that when buttons are pressed in the virtual world, the related actions are called and activated on the hardware side.

The player avatar model consists of hands tracked by the headset controllers that allow them to interact with the buttons within the environment just like in real life. Players can also freely move around to closely interact with digital twin components, creating a sense of physical presence at the water treatment facility.

We used a water program from the Unity asset store that uses C# programming to create realistic physics properties of the water within the virtual environment. Accurate movement and flow direction of the water can be seen as different components of the water treatment plant are turned on and off to simulate real-life behavior. On top of that, we also added capabilities to the water color so that dirty water is portrayed as purple at the beginning of the water treatment process and as the water filtration is taking place the water color becomes blue to signify clean water.

During the development of the XR environment, we ran into several challenges. One issue that arose was the issue of merging scenes. As the project builds upon previous work, we had to keep in mind the existing XR environment and design which had their player design aspect. This meant it would be

difficult to create a new interactive player with a different script and interaction technique since it would not be compatible with the existing environment. To resolve this issue we used prefabs (preconfigured digital assets) for development that allowed us to integrate the player into the environment seamlessly.

Another challenge we faced was Print Mesh Rendering. When we tried to display real-time data from each chamber in the VR environment, we encountered difficulties. We aim to address and resolve this issue moving forward.

6 Qualitative Evaluation

We completed a guided tour of a Water Treatment plant in Roanoke, Virginia where we learned about the water treatment process and the current status of their cybersecurity systems from plant workers. Plant workers walked us around the plant showing the computer systems involved in each treatment process and how it connects to their network. During the visit, we observed flaws in the physical aspects of the plant. Many of the computer systems within the plant were not secured within a locked room, meaning any plant worker could gain access to it physically. We noticed that the filtered water is directly reintroduced into the stream, implying that any malfunction in the water treatment process could lead to immediate environmental repercussions. This risk is magnified due to the direct connection of the stream to a significant river, which, in turn, connects to various other bodies of water. Seizing the opportunity, we also conducted interviews with multiple staff members at the plant to inquire about their cybersecurity backgrounds and the precautions they take to prevent cybersecurity attacks during their work at the facility.

6.1 XR Environment

We have designed a virtual model of a water treatment plant that contains all of the components that mimic each stage of the water treatment process. Screenshots of the virtual environment have been provided in Fig. 3. the tiny cylinders that you see in the world are the acids, bases, and organisms that would be added to the water at each step of the system. Users can walk along the platform or below the platform to provide that immersive feeling of being at the actual plant.

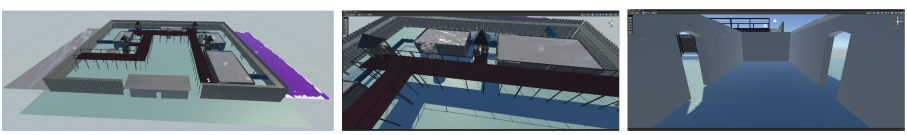

Fig. 3. Left: Sky view of Water Treatment Plant. **Middle:** Zoomed in view. **Right:** User's point of view.

6.2 Physical AI Agent

We were able to classify our 3 different attack classes using LangChain. By providing a high-level description of what the attack is doing, we can classify the specific cyberattack that is occurring.

As demonstrated in Fig. 4, we provided a high-level attack description describing that the network speed for the water treatment speed is slow due to there being so much traffic. An attack template is created that provides specific instructions on how the LLM should evaluate the given description along with how the LLM should return the output.

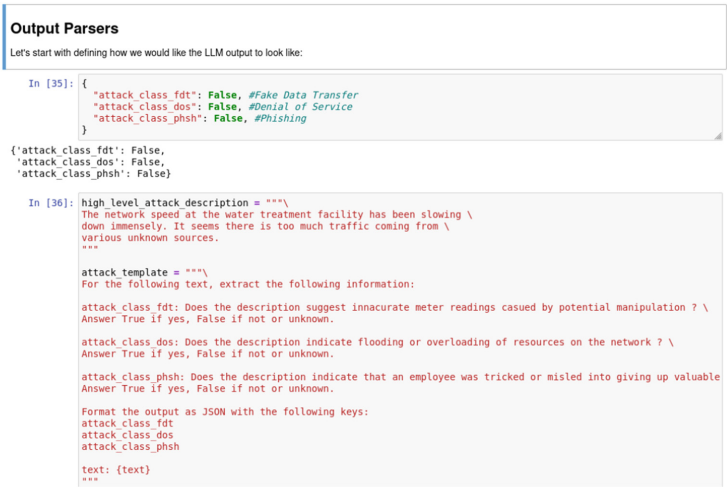

Fig. 4. Langchain prompt implementation.

We decided to use a JSON containing a boolean as output so that we could easily determine which attack script to execute. The resulting output from the LLM can be seen in Fig. 5.

We can see that the high-level attack description was successfully classified as a Denial of Service attack. The other two attack classes were also successfully classified as shown in Fig. 6.

The attack script for the Denial of Service attack class was successfully created in Python using the OpenAI and the llama_cpp library. The attack script produces a Python list containing flooding commands for each network of interest that can then be fed and executed on our testbed's command line interface. The next step would be for us to apply the commands on the testbed's network to see the results.

Fig. 5. LLM's Response given a Denial of Service attack description.

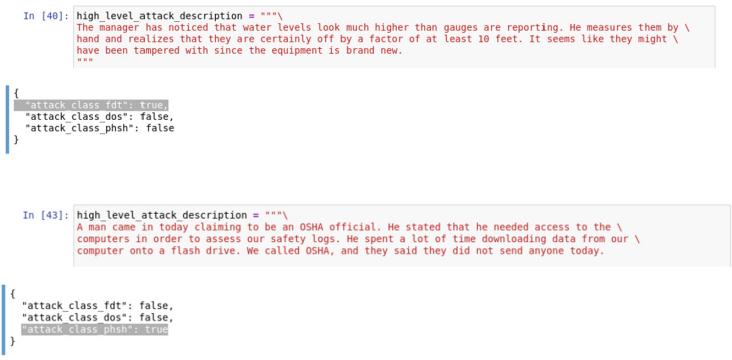

Fig. 6. Top: LLM's Response given a Data Manipulation attack description. **Bottom:** LLM's Response given a Phishing attack description.

7 Conclusions and Future Work

We introduced a novel XR-based testbed that integrates AI and LLMs to create an immersive educational experience that addresses the need for proper cybersecurity training among water treatment plant employees. The testbed provides users with a real-world representation of the potential outcomes resulting from successful cyber attacks. Our goal is to enhance the educational process and promote a deeper understanding of cybersecurity challenges in critical infrastructure like water treatment plants.

In the future, we plan on taking information from the IoT devices to create visuals for the statistics of each chamber of the water treatment system for easy readability and understanding for the user while interacting with the XR. Without the statistics being presented in the XR environment, they would have to rely on the front-end interface for the statistics. We are also planning

to address *Conversational AI NPC* interaction issues within VR, enabling the use of the Meta Quest headset for interactions. Additionally, we aim to optimize AI responses in correlation with the XR environment to facilitate real-time AI connections and synchronized NPC movement.

Acknowledgment. This study is a collaboration between Virginia Tech and Virginia Military Institute (VMI) as a part of a Commonwealth Cybersecurity Initiative Workforce Development Grant. A great many thanks to the cadets at VMI for helping us implement XR environment and the attack and defense scenarios for the testbed simulation.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Balaji: HPING3 — network scanning tool — packet generator (2023). https://gbhackers.com/hping3-network-scanner-packer-generator/. Accessed 2 Feb 2024
2. Bomey, N.: How Chinese military hackers allegedly pulled off the equifax data breach, stealing data from 145 million americans (2020). https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/. Accessed 2 Feb 2024
3. Chandrashekar, N.D., King, K., Gračanin, D., Azab, M.: Design & development of virtual reality empowered cyber-security training testbed for IoT systems. In: 2023 3rd Intelligent Cybersecurity Conference (ICSC), pp. 86–94 (2023). https://doi.org/10.1109/ICSC60084.2023.10349976
4. Chandrashekar, N.D., Safford, S., Muniyandi, M., Gračanin, D.: An extended reality simulator for pulse palpation training. In: 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), pp. 178–182 (2023). https://doi.org/10.1109/VRW58643.2023.00044
5. Chase, H.: Langchain (2022). https://www.langchain.com/. Accessed 2 Feb 2024
6. Easterly, J., Fanning, T.: The attack on colonial pipeline: what we've learned & what we've done over the past two years: CISA (2023). https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Accessed 2 Feb 2024
7. Francis, N., Ante, J., Helgason, D.: Unity real-time development platform | 3D, 2D, VR & AR. Unity Technologies (2005). https://unity.com/. Accessed 2 Feb 2024
8. Gironacci, I.: XR management training simulator supported by content-based scenario recommendation. In: 2022 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), pp. 104–108 (2022). https://doi.org/10.1109/AIVR56993.2022.00021
9. Hertel, J.P., Millis, B.: Using Simulations to Promote Learning in Higher Education: An Introduction. Routledge, London (2002)
10. Jobbins, T.: Thebloke/luna-ai-llama2-uncensored-gguf at main (2023). https://huggingface.co/TheBloke/Luna-AI-Llama2-Uncensored-GGUF/tree/main. Accessed 2 Feb 2024

11. Korodi, A., Nicolae, A., Drăghici, I.A.: Proactive decentralized historian-improving legacy system in the water industry 4.0 context. Sustainability **15**(15) (2023). https://doi.org/10.3390/su151511487
12. Lyon, G.: Nmap: networking security scanner (1997). https://nmap.org/. Accessed 2 Feb 2024
13. Nagarajan, A., Allbeck, J.M., Sood, A., Janssen, T.L.: Exploring game design for cybersecurity training. In: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256–262 (2012). https://doi.org/10.1109/CYBER.2012.6392562
14. Ono, T., Ishikawa, T.: A research on penalty kick training system using XR. In: 2023 Nicograph International (NicoInt), pp. 86–86 (2023). https://doi.org/10.1109/NICOINT59725.2023.00026
15. Shapira, N., Ayalon, O., Ostfeld, A., Farber, Y., Housh, M.: Cybersecurity in water sector: stakeholders perspective. J. Water Resour. Plan. Manag. **147**(8), 05021008 (2021). https://doi.org/10.1061/(ASCE)WR.1943-5452.0001400
16. Sutskever, I.: (2023). https://openai.com/gpt-4. Accessed 2 Feb 2024
17. Yoshida, S., Abe, T., Suganuma, T.: Design of a support system for guitar performance training using XR technology. In: 2023 IEEE 12th Global Conference on Consumer Electronics (GCCE), pp. 276–279 (2023). https://doi.org/10.1109/GCCE59613.2023.10315398