A STUDY OF BUILDING INTELLIGENT SYSTEMS USING REINFORCEMENT LEARNING FOR REMOTE INSTRUMENTATION AND IMMERSIVE LEARNING

ANIRUDH KAMBHAMPATI

Prasad Calyam

JULY 2024

BUILDING INTELLIGENT SYSTEMS USING REINFORCEMENT LEARNING FOR REMOTE INSTRUMENTATION AND IMMERSIVE LEARNING

presented by Anirudh Kambhampati,

Prasad Calyam

Filiz Bunyak

Noah Glaser

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my mentor, Dr. Prasad Calyam, for his unwavering support, insightful advice, and steadfast guidance throughout my thesis journey. His dedication to academic excellence and fostering a curious mindset has greatly influenced my academic path. This thesis is a testament to the collaborative spirit and perseverance that defines our lab's efforts.

I am incredibly grateful to be a part of the VIMAN and CERI labs. The vibrant and collaborative atmosphere within these labs has significantly contributed to my personal and professional growth. The success of this thesis is a reflection of the dedication and enthusiasm of the exceptional individuals in these dynamic research communities.

I extend my heartfelt thanks to my fellow lab members. Your friendship, constructive feedback, and invaluable insights have been greatly appreciated. Your support and encouragement have been a constant source of strength. The achievements and reflections in this thesis are a result of our shared journey of learning and relentless pursuit of knowledge.

I would also like to acknowledge the faculty and staff of the department for their essential resources and guidance, which have been instrumental in the completion of this thesis. Your unwavering commitment to fostering an environment of academic excellence has profoundly impacted my work.

Furthermore, I am deeply thankful for the mentorship of Dr. Noah Glaser and his team at the IE lab. Their guidance and support have been invaluable to my research and development.

Lastly, I am immensely grateful for the steadfast love and encouragement from my parents, family members, and friends. Their unwavering support has enabled me to tirelessly work towards the successful completion of this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

ABSTRACT

Reinforcement Learning (RL) has the potential for developing intelligent, adaptive systems and foster feedback-oriented training of software to make decisions that maximize rewards, and increase accuracy of outcomes. However, challenges such as the complexity of real-time analysis in dynamic environments, ensuring data quality and diversity for robust training, and making RL models interpretable for stakeholders present unique research challenges. In this thesis, we explore the design and implementation of RL-based algorithms to develop intelligent systems within two distinct domains: (i) remote instrumentation for intelligent image analytics in materials manufacturing, and (ii) virtual reality for intelligent pedagogical assistance in immersive cybersecurity education.

In the first domain, we present the design of an intelligent system for real-time image processing tasks in a cloud-based platform designed to automate and optimize the process of image analytics in scientific experiments. Specifically, we develop a Remote Instrumentation Science Environment (RISE) platform that integrates remote instruments and data centers using cloudlets, providing seamless access through a high-level language API. By employing RL agents, RISE enables real-time analysis and dynamic adjustment of instrument settings enhancing experimental control. In the second domain, we present the design of an intelligent Pedagogical Agent (PA) to support adaptive learning experiences in a Virtual Reality Learning Environment (VRLE), "CyEscape". Integrating Deep Q-Network with OpenAI and Unity, the PA is trained on guiding the learners through a dynamic learning environment, featuring escape rooms that create a practical and immersive approach to cyber security education.

Through validation experiments of RISE and CyEscape, we highlight the transformative potential of RL in creating intelligent systems that are adaptive, and user-centric to improve pace of discovery in image analytics, and educational outcomes in cybersecurity training.

Chapter 1

INTRODUCTION TO INTELLIGENT SYSTEMS WITH REINFORCEMENT LEARNING

Reinforcement Learning is a branch of machine learning where an agent learns to make decisions by performing actions in an environment to achieve some notion of cumulative reward. This paradigm is inspired by behavioral psychology, where learning is driven by the consequences of actions. Unlike supervised learning, where the model is trained on a fixed dataset, RL involves an agent that must explore and exploit the environment to gather data, learn from it, and make increasingly better decisions.

The RL framework typically consists of states, actions, rewards, and a policy. The state represents the current situation of the environment, the action is what the agent can do, the reward is the feedback from the environment in response to the action, and the policy is the strategy that the agent employs to decide the next action based on the current state. One of the fundamental algorithms in RL is Q-Learning, which aims to learn the value of action in a particular state, helping the agent to choose actions that maximize the expected cumulative reward.

The potential of RL is vast, with applications ranging from robotics and autonomous vehicles to healthcare and finance. In robotics, RL can be used to teach robots to navigate complex environments or manipulate objects with high precision. In autonomous vehicles, RL algorithms enable cars to make real-time decisions in dynamic traffic conditions. In healthcare, RL has the potential to optimize treatment plans and improve patient outcomes by learning from historical data and patient responses. In finance, RL can be used to develop trading strategies that adapt to market changes. By learning from interactions within an environment, RL algorithms can optimize performance over time, making them particularly suitable for complex, dynamic tasks. Despite its potential, several challenges need to be addressed to harness the full capabilities of RL. These challenges include the complexity of

real-time analysis in dynamic environments, ensuring data quality and diversity for robust training, and making RL models interpretable for stakeholders. This thesis delves into these challenges, exploring the design and implementation of RL-based algorithms to develop intelligent systems within two distinct domains: remote instrumentation for intelligent image analytics in materials manufacturing, and virtual reality for intelligent pedagogical assistance in immersive cybersecurity education.

However, deploying RL in real-world applications presents several challenges. One major challenge is the need for large amounts of high-quality data to train RL models effectively. In many real-world scenarios, collecting sufficient data can be expensive and time-consuming. Additionally, RL models often require significant computational resources for training, which can be a barrier for many organizations. Another challenge is the interpretability of RL models. Since RL involves complex decision-making processes, it can be difficult to understand and explain why a model makes certain decisions. This lack of transparency can be a significant hurdle for gaining stakeholder trust and ensuring ethical use of RL systems.

Given the complexity and potential of RL, this thesis explores the design and implementation of RL-based algorithms to develop intelligent systems within two distinct domains: remote instrumentation for intelligent image analytics in materials manufacturing, and virtual reality for intelligent pedagogical assistance in immersive cybersecurity education.

In the first domain, the focus is on the development of a Remote Instrumentation Science Environment (RISE) platform. This platform leverages cloud-based technology to integrate remote instruments and data centers using cloudlets, providing seamless access through a high-level language API. By employing RL agents, RISE enables real-time image processing and dynamic adjustment of instrument settings, enhancing experimental control and optimizing the process of image analytics in scientific experiments.

In the second domain, the thesis explores the development of an intelligent Pedagogical Agent (PA) within a Virtual Reality Learning Environment (VRLE) called "CyEscape". This VRLE is designed to provide an immersive cybersecurity training experience through escape room scenarios. The PA, integrated with Deep Q-Network and powered by OpenAI and Unity, guides learners through the dynamic learning environment, offering adaptive support and feedback to improve educational outcomes.

The primary contributions of this thesis are twofold. First, it presents the design and implementation of the RISE platform, demonstrating how RL can be used to enhance real-time image analytics in materials manufacturing. Second, it introduces the intelligent Pedagogical Agent in

the CyEscape VRLE, showcasing the potential of RL to create adaptive, user-centric educational experiences. Through validation experiments, the thesis highlights the transformative potential of RL in both scientific and educational domains, emphasizing its ability to improve the pace of discovery in image analytics and enhance learning outcomes in cybersecurity training.

The remainder of this thesis is organized as follows. Chapter 2 provides a comprehensive review of the literature on RL, its applications, and the specific challenges associated with real-time analysis, data quality, and interpretability. Chapter 3 details the design and implementation of the RISE platform, including the integration of RL agents for real-time image processing. Chapter 4 discusses the development of the intelligent Pedagogical Agent in the CyEscape VRLE, describing the integration of Deep Q-Network and the immersive learning environment. Chapter 5 presents the validation experiments and results, demonstrating the effectiveness and impact of the proposed systems. Finally, Chapter 6 concludes the thesis, summarizing the findings and discussing potential future research directions.

Through the exploration of RL in these two domains, this thesis aims to contribute to the development of intelligent systems that are not only adaptive and efficient but also user-centric, paving the way for advancements in both scientific research and education.

Chapter 2

RELATED WORKS

2.1 Remote Instrumentation and Image Analytics

2.1.1 Remote Instrumentation Control

There have been significant efforts to improve the resource efficiency of scientific instruments through remote instrumentation. One notable example is the BRACELET framework, introduced by Nguyen et al. [1], which uses an edge-cloud microservice approach to address performance and security challenges while enabling remote access. Central to BRACELET is the concept of a cloudlet, serving as an intermediary between scientific instruments and a cloud-based analytics service, thus resolving issues like network bandwidth limitations and firewall restrictions. Similarly, Calyam et al. [2] proposed the Remote Instrumentation and Collaboration Environment (RICE), which focuses on multi-user remote access and collaboration in scientific image analytics, overcoming network bottlenecks.

Our work on the RISE platform builds on these foundational efforts. By incorporating cloudlet technology and focusing on performance and security, RISE enhances remote instrumentation with a chatbot-guided interface and a suite of web services. This approach aims to reduce workflow durations, improve resource utilization, enhance image analytics accuracy, and lessen the dependency on specialized expertise.

2.1.2 Learning-Based Approaches for Feedback Control

Combining remote instrumentation with learning-based feedback control has shown significant benefits. For instance, Hajilounezhad et al. [3] used a deep learning model trained on synthetic data to predict properties of CNT materials synthesized on SEMs. However, the challenge remains in constructing

similar models from real SEM images due to limited data availability. In optimization-based model predictive control (MPC), studies like Ahn et al. [4] have adopted Imitation Learning (IL) to leverage the structural nuances of constrained linear MPC, achieving optimal performance.

Recent studies have demonstrated the effectiveness of Multi-Agent Deep Deterministic Policy Gradient (MADDPG) in various control tasks, such as providing real-time protection for smart grids [5] and power control in fog computing networks [6]. These successes underscore MADDPG's potential in control and optimization scenarios, making it suitable for tasks like CNT image segmentation and characterization.

Our work compares RL and IL agent-based approaches to determine the optimal algorithm for guiding real-time image processing in CNT manufacturing using SEMs. We extend previous efforts by employing a MADDPG-based method for generating feedback commands, improving scanned image quality, and utilizing IL techniques to mimic expert actions in SEM setup. The integration of learning algorithms with a chatbot-based service allows users to interface with cyber-enabled instruments, transforming manual CNT manufacturing processes into more efficient, error-free workflows.

2.1.3 Image Analytics Automation

Automation in data analysis and instrument control has been a focus of several previous works. Nguyen et al. [7] proposed the 4CeeD framework for real-time data collection and coordination in scientific instrumentation, while the Smartscope framework [8] automates cryo-electron microscopy grid screening. The AI-AFM system [9] provides real-time pattern recognition in atomic force microscopy, reducing human intervention.

Our approach in RISE aligns with these objectives by employing a chatbot-guided interface for dynamic image quality adjustments using RL techniques. Inspired by chatbot-based systems like HAICO [10], our interface enhances user experience by automating instrument settings and integrating security mechanisms to ensure data and network access security.

2.2 Virtual Reality and Cybersecurity Education

2.2.1 Adaptive VR Learning Environments

Game-based learning in adaptive VR environments harnesses the inherent motivation of play to foster engagement, collaboration, and problem-solving skills [11, 12]. Adaptive VR Learning Environments (VRLEs) enhance these benefits by tailoring experiences in real-time using procedural content

generation algorithms [13], optimizing learning outcomes, and fostering deeper engagement [14].

Escape Rooms implemented in adaptive VRLEs, such as CyEscape, replicate the immersive qualities of physical escape rooms [15]. By utilizing an RL-based Pedagogical Agent (PA), CyEscape addresses scalability and retention challenges, providing realistic cybersecurity incident scenarios and personalized feedback [16]. This approach ensures a sophisticated learning experience, transcending traditional models.

2.2.2 Cybersecurity Training in VR

Traditional educational approaches often fall short in providing hands-on training for real-world cybersecurity challenges [17]. VR games fill this void by immersing learners in realistic scenarios [18], covering tasks like vulnerability identification and system patching in a risk-free setting [19]. Initiatives like GenCyber summer camps highlight VR's potential in cybersecurity education [20, 21].

CyEscape advances cybersecurity education by integrating insights from existing initiatives. It provides a dynamic framework for learners to engage in authentic cybersecurity tasks, combining game-based learning principles to ensure comprehensive skill development. By emphasizing inclusivity and collaborative learning, CyEscape offers structured and visually appealing VR environments that promote interdisciplinary collaboration [22].

2.2.3 Pedagogical Agents in VR

The inclusion of PAs in VR environments is pivotal in educational research, offering dynamic opportunities and challenges [23, 24, 25]. Studies have emphasized the significance of defining clear roles for these agents, such as Expert, Motivator, and Mentor, ensuring engagement and effectiveness [26, 27]. Reviews have highlighted the impact of agent appearance and role on learning outcomes, providing valuable insights for designing effective agents [28].

CyEscape integrates a PA driven by RL to provide personalized guidance and feedback, adapting in real-time to individual learner needs. By employing a backward design approach, CyEscape iterates on curriculum design to ensure alignment with learning objectives, enhancing educational effectiveness. This novel approach not only boosts learner engagement but also equips them with the skills to effectively tackle evolving cyber threats.

Overall, these related works provide a comprehensive foundation for our research. By building on previous efforts in remote instrumentation, image analytics automation, and VR-based education, we aim to contribute significantly to these fields, demonstrating the transformative potential of RL and

adaptive learning technologies.

Chapter 3

METHODOLOGY

3.1 RISE: Remote Instrumentation Science Environment for Learning-based Image Analytics

Scientific workflows, particularly in fields such as materials development, involve laborious environment setup and operation, data-intensive processes, and intricate data analysis tasks. For example, in carbon nanotube (CNT) forest synthesis using a scanning electron microscope (SEM) [29, 2], researchers must determine optimal image scanning parameters (e.g., zoom, focus, contrast) through manual calibration, data acquisition and transfers to data centers, and iterative image analysis [30, 31]. Moreover, in CNT forest synthesis, real-time control of the growth rate is crucial for achieving desired material properties, requiring immediate identification of the current growth rate and prediction of necessary parameter updates [32]. Manual execution of these processes poses challenges such as labor intensity, reliance on trial-and-error methods, and delays in gaining insights. Moreover, collected datasets often involve multi-dimensional parameters [29, 3], demanding specialized analytical tools for timely interpretation. The reliance on conventional manual approaches prolongs experimentation timelines and increases the likelihood of errors and inconsistencies.

Image characterization and CNT growth control are crucial in CNT synthesis research as they directly impact the quality and characteristics of the synthesized materials. Real-time monitoring and adjustment of SEM parameters are desirable for steering experiments toward expected outcomes. The implementation of automated processes to aid users in SEM setup, data collection, and swift analysis of CNT images can enhance decision-making capabilities and improve experimental results. Such automation can streamline workflows, reduce manual tasks, and facilitate the prompt generation of feedback commands to optimize experimental results. To tackle the issues of manual instrument

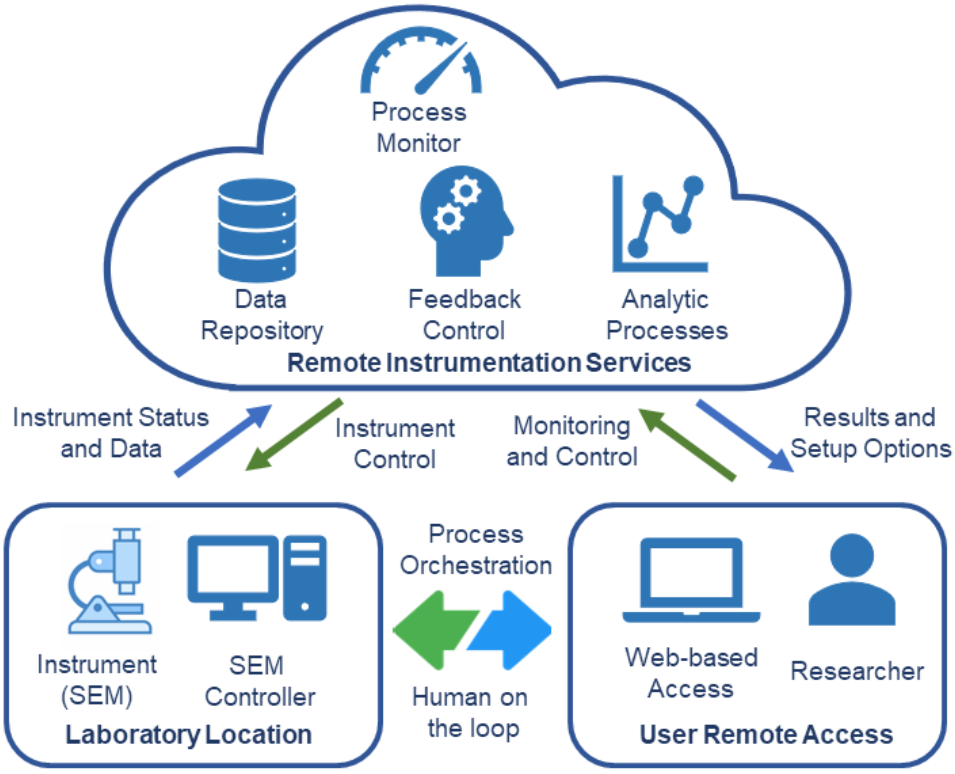


Figure 3.1: Illustration of remote instrumentation with automated feedback to assist in image analytics and overcome limitations in manual processes.

access, setup, and control, as well as the complexities of data collection and real-time analysis needs in scientific experiments, a comprehensive solution is required.

Leveraging remote instrumentation, automated data management, and ML-based methods can significantly reduce manual effort and streamline experimentation. Real-time data collection and analysis, coupled with immediate feedback generation for instrument setup updates, enables a closed-loop experimentation control approach as depicted in Figure 3.1. Closed-loop automated instrument control, demonstrated in prior studies [33, 34], ensures efficient operation, particularly beneficial for novice users navigating critical SEM settings like those for growing CNTs. However, realizing the full potential of remote instrumentation poses challenges. Firstly, integrating various scientific instruments seamlessly, securely, and with proprietary interfaces remains a challenge. Secondly, automated image collection, transfer, storage, and management of large datasets in diverse storage technologies present logistical hurdles. Thirdly, implementing effective real-time data analytics methods, particularly ML-based approaches, requires substantial image volumes and varied experiment setups for model training. Current CNT synthesis experiments are manually exhaustive and time-consuming, limiting meaningful results suitable for ML-based training. Lastly, orchestrating iterative workflows in scientific experiments, where intermediate images guide subsequent instrument adjustments, demands

seamless automation and secure remote control.

In this thesis, the above challenges are adressed by proposing a Remote Instrumentation Science Environment (RISE). RISE features cloud-based services for collecting images from CNT growth experiments and automates feedback control on the SEM to improve image quality. Inspired by two CNT synthesis experiments [29, 3], the aim is to optimize the zoom, focus, and contrast of CNT images. RISE leverages advanced technologies such as web services, cloud computing, and machine learning-based methods to connect SEM instruments and storage units via cloudlets and high level APIs. This structure enables the global collection of CNT images, execution of image analytics, and implementation of feedback control. A distinctive feature of RISE is its integration of machine learning, specifically reinforcement learning (RL), for iterative optimization of instrument settings. This approach enhances image analytics accuracy. The RL agents embedded within the system provide real-time feedback control of the microscope using image analytics outputs, reducing time spent on microscope control and minimizing operational errors. This enables researchers to receive real-time feedback and optimize experimental parameters. However, existing cloud-based solutions often address specific sub-problems within instrument-based scientific workflows, lacking the ability to automate the entire workflow using AI/ML and provide real-time guidance to researchers based on analytics outputs. Such guidance can aid in adjusting microscope settings or optimizing image parameters during imaging, thereby saving researchers time and valuable microscope resources.

Through experiments, a comparative performance analysis of RL with another ML algorithm Imitation Learning (IL) under dynamic conditions using 236 CNT images captured in SEM experiments is conducted. The experiments involved configuration of preliminary scanning parameters on the SEM before capturing initial images. Subsequently, the acquired CNT images are subjected to a segmentation pipeline, employing the CNTSegNet [35] model — a dual loss, orientation-guided, self-supervised, deep learning network — to identify and segment CNT elements. Following segmentation, we compare the results with the RL and IL agents to evaluate which optimizes the scanning parameters to enhance image quality. Particularly, the performance of the agents in predicting Zoom, Focus and Contrast parameter selections using labeled data for offline training to guide the navigation of dynamic adjustments in SEM instrument settings is compared. To ensure result accuracy, our evaluation is limited to authentic CNT images, excluding synthetic or programmatically modified ones. Obtaining suitable CNT images through practical experimentation is challenging, and hence we rely solely on the available 236 CNT images deemed appropriate for our study.

The remainder of the RISE is organized as follows: . In Section 3.1.1, CNT characterization process workflow involving image segmentation is detailed. In Section 3.1.2, the learning-based SEM

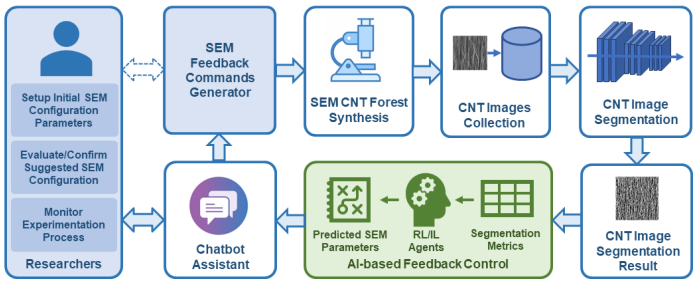


Figure 3.2: Illustration of the CNT images segmentation workflow and SEM feedback control mechanism in the Remote Instrumentation Science Environment.

instrument control approach using RL algorithm is described. Section 3.1.3 presents the RISE web service architecture along with implementation details. Section 3.1.4 compares the performance of the RL/IL algorithms in a realistic cloud-based testbed. Section 3.1.6 concludes the RISE section of this thesis.

3.1.1 CNT Image Analytics and Characterization Background

This section delineates the analysis and characterization of CNT synthesis images integrated into our RISE system. This use case serves to validate our SEM ML-based feedback control and the human-in-the-loop experimental process orchestration.

Effective evaluation of partial experiment results and timely prediction of updated instrument parameters for feedback command generation are essential yet challenging to achieve [3]. Overcoming these challenges can establish an integrated scientific experimentation environment, where networked instruments provide remote access for sample preparation, configuration, image collection, transfer, storage, and ML-based analysis. Additionally, web services and guided user interfaces facilitate convenient, secure remote instrument control, fostering collaboration and accelerating scientific discoveries. Here, a CNT manufacturing use case that benefits from such remote instrumentation and real-time calibration approach using AI-based agents following accurate image segmentation is introduced. This specifically discusses how user-AI agent interaction can be utilized to predict and recommend Zoom, Contrast, and Focus parameters in image acquisition tasks.

The process of growing CNT forests requires extensive preparation for in-situ experiments. Human insight is crucial to achieving desired material characteristics. High-quality images are valuable for evaluating the CNT forest structural morphology, but manual SEM scanning parameter adjustments are often time-consuming and can be error-prone due to trial-and-error. This is particularly true for novice SEM users. A dynamic setup recommendation system that optimizes SEM parameters given the latest scanned image would expedite image acquisition, reduce the need for human intervention

and enhance CNT forest characterization processes significantly.

Figure 3.2 illustrates our Remote Instrumentation Science Environment (RISE) solution that features a closed-loop mechanism involving the CNT segmentation process using the CNTSegNet [35] deep learning pipeline. The initial scanning parameters are set by the CNT manufacturing users through the SEM command controller using a web-based user interface that includes a chatbot agent. This approach employs natural language communication to provide users with the results of system inferences and interpret their actions about the changes on the SEM parameters. CNT images are processed using segmentation powered by ML models in CNTSegNet for CNT identification. Metrics from segmented images (i.e., Orientation Loss, Edge Coverage, Average Thickness, Average Separation, and Distance Entropy) guide RL/IL agents in predicting optimized image scanning parameters (i.e., Zoom, Focus, Contrast) [36].

In addition, the chatbot agent suggests new parameters based on the characterized SEM image parameters, and upon user confirmation, the chatbot relays the parameters to the SEM command controller for instrument adjustment and execution of new image scanning. This adjustment process continues iteratively until CNT manufacturing users are satisfied with the image quality, ensuring that subsequent experiment images are captured with the latest confirmed scanning parameters. Alternatively, users can directly interact with the SEM controller through a user interface for manual control, when immediate action is needed. By utilizing the chatbot agent's assistance, users can explore additional options to configure SEM parameters without being constrained by a fixed set of values. They can also do so without the concern of applying values beyond reasonable limits, as the chatbot agent interacts with users to communicate the potential outcomes of their selections.

3.1.2 Learning-based CNT Image Segmentation and Characterization

In this section, the RL-based instrument control approaches, designed to address the challenges of time-consuming and error-prone manual instrument control is detailed. This is particularly relevant for novice users adjusting instrument settings during CNT image collection. Given the limited size of the training dataset, our goal is to identify the most effective methods for image analysis. RL/ Multi-agent RL (MARL) particularly suitable for this task as they excel in learning and adapting from small datasets by leveraging expert demonstrations and iterative improvements. This allows us to optimize the accuracy and efficiency of CNT image segmentation and characterization within our RISE system.

RL-based CNT Image Characterization

RL-based Model Description

The instrumentation control process involves optimizing a decision-making process with five input parameters (Orientation Loss, Edge Coverage, Average Thickness, Average Separation, and Distance Entropy) used to determine three distinct setup action values (Zoom, Focus, Contrast). The objective is to determine the best action values, in order to achieve the best possible settings for an SEM to obtain ideal CNT images. This decision-making task poses a challenge due to the complex multi-input and multi-output nature of the CNT manufacturing problem.

For our first ML-based image analytic approach, the MADDPG [37]; an RL environment designed to achieve optimal feature selection using the available data was explored. In our scenario, multiple agents interact with the data to achieve desired correlations between features, thereby producing the best possible settings for the SEM. MADDPG is well-suited for this task as it excels in decentralized Multi-Agent Reinforcement Learning (MARL) settings. Here, agents such as the zoom agent, focus agent, and contrast agent have independent roles and can influence the environment only through their actions. MADDPG is adept at handling continuous action spaces, which is essential since all the values in our data are continuous. The algorithm facilitates effective coordination among agents and employs an actor-critic architecture: the actor network proposes actions for each agent, while the critic network evaluates the collective performance of all agents. This combined approach, along with a memory buffer, helps agents develop effective policies to achieve the overall goal of maximizing desired correlations.

In traditional MADDPG frameworks, agents typically exchange raw observation or action values during training, resulting in high-dimensional input spaces. This is conspicuous in our setting as the parameter ranges are diverse. Therefore, by leveraging correlations between the image scanning parameters: zoom, focus and contrast and image parameters: orientation loss, edge coverage, average thickness, average separation, and distance entropy, the unique challenges posed by the diverse range of values encountered in our problem domain is addressed . Using correlations to capture the intricate interactions between scanning and image parameters ensures that agents can efficiently represent the underlying dynamics of the environment without relying solely on the raw values, which may vary significantly in magnitude and scale.

Considering the five image parameters in space, the three agents iteratively select pertinent values, aiming to minimize the difference between the actual correlation and the observed correlation in the environment, thereby increasing rewards. As a Markov's process, learning space is defined as $\{s_t,$

a_t, r_t, $s_{t+1}\}$ where $s_t \in \mathcal{S}$ is the current state holding the correlations among variables, $a_t \in \mathcal{A}$ is the action that influences the state. Here, multiple agents take different actions in the environment recommending better settings over iterations, $r_t \in \mathcal{R}$ is the reward received by the agents and $s_{t+1} \in \mathcal{S}$ is the state the environment has transitioned to after an action is taken. Below the elements of our RL environment is described.

State space: The state space encompasses the possible states or observations that the environment can provide to the agents. It is defined for each agent as a vector of length 5, representing the correlations of the Zoom, Focus, and Contrast with Orientation Loss, Edge Coverage, Average Thickness, Average Separation, and Distance Entropy. Each state S_t for t^{th} agent can be represented as:

$$S_t = (c_1, c_2, c_3, c_4, c_5)$$

Where c_j represents the correlation coefficient of the j^{th} observed image parameter with the scanning parameters.

Action space: This Markov's Decision Model considers each agent taking a set of actions $(\mathcal{A}_1, ..., \mathcal{A}_N)$, and states $(S_1, ..., \mathcal{S}_N)$ in our environment. Each agent takes a policy π_θ such that $\pi_{\theta_t} \rightarrow \mathcal{S}_t \times \mathcal{A}_t$ generating the next state for the environment. Each agent takes the current state as an input of tensors and pass through the actor network to generate an action. A Gaussian noise is added to the action to improve the exploration.

Reward function: The reward function defines the immediate feedback that an agent receives for taking a particular action in a given state. Let $\mathcal{R}_t$ denote the reward received by agent t for a particular action. Each agent strives to maximize its cumulative expected reward over time. The reward function $\mathcal{R}_t$ can be defined as:

$$\mathcal{R}_t \rightarrow \mathcal{S} \times \mathcal{A}_t$$

RL-based CNT Image Parameters Prediction

Algorithm 1 implements our MADDPG in a MARL setting to optimize image scanning for real-time calibration. This algorithm trains our agents to learn an optimal policy for predicting instrument setup parameters. The segmentation parameters are used as features to evaluate the quality of the image, providing information about the performance of the image processing algorithm based on the chosen parameters. The environment provides feedback in the form of rewards based on the agent's actions taken in each state. The algorithm iteratively explores the environment, refines its actions, and converges to an optimal solution over time. Our RL agent code is available here [38].

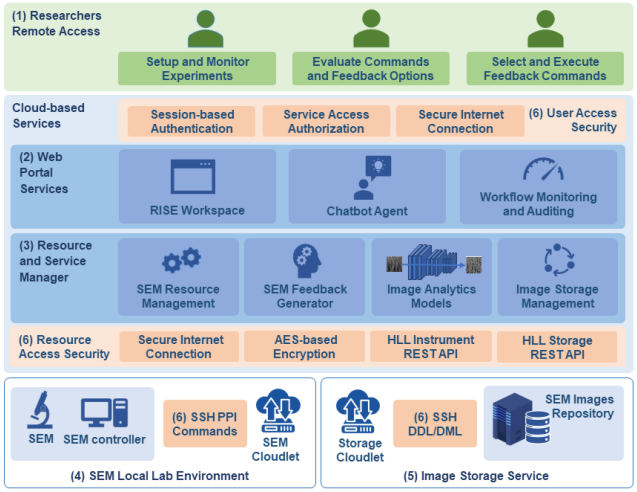


Figure 3.3: RISE web services architecture components.

In our RL environment setup, the number of actions available is initially the same for all agents, eliminating the need for padding later. However, the environment conveniently selects only the actions required to make a decision.

Algorithm 1: MADDPG algorithm to recommend optimal instrument parameters

Require: Dimensions for actor and critic networks with the number of agents and number of actions available for each agent.
Ensure: Initialize the actor network with a *tanh* activation selecting optimal hyperparameters α, β and τ and define the memory buffer.

Initialize environment and MADDPG agents
Initialize replay buffer memory
for i **in** $[1, N\_GAMES]$ **do**
    Reset environment to initial state and get initial observations *obs*
    while None of the agents are done **do**
        actions = $maddpg.choose(obs)$
        actor = **actor_network**$(\alpha, actor\_dims, actions)$
        critic = **critic_network**$(\beta, critic\_dims, actions)$
        Executes actions $\mathcal{A} = (\mathcal{A}\_1(t), ..., \mathcal{A}\_1(t))$ in the environment Pass the Actions to modify the environment
        memory.store_transition(obs,state,action,reward) Updates state and next state arrays with the new values
        maddpg_agents.learn(memory) Calculate *Critic Network and Actor Network* for each agent and update loss
    end while
    total_reward.append(episode_score)
end for

3.1.3 RISE Web Service Architecture

In this section, the six key components of the RISE web services architecture shown in Figure 3.3 is detailed featuring: (1) remote user access to experiment workspace; (2) web portal services for users to monitor workflows and interact with the chatbot guided interface; (3) back-end services providing AI/ML-based feedback during image analytics experiments; (4) integration with local lab instrumentation environment integrated via a cloudlet; (5) storage service integrated via a cloudlet; and (6) resource access security mechanisms between SEM, storage repositories, and their respective cloudlets.

Researcher Remote Access

The Researcher Remote Access component enables researchers to access the web service, providing them with the capability to configure and oversee experiments using the chatbot agent. Additionally, it facilitates the evaluation of SEM commands and feedback commands, empowering researchers to select and modify SEM commands for executing new SEM experiments. Through the web services, researchers engage with the user interface to initiate actions. The progress and status of experiments are tracked in a command-line style window. Users can choose from existing, raw images or upload images from their local computers for analysis. The image analysis process prompts a reinforcement learning (RL) based chatbot guidance [39] to generate suggestions for improved experiment outcomes. Upon the researcher's execution or acceptance of these new recommendations, a fresh experiment setup is prepared. This setup can be monitored within the web service, displayed in a command-line format window.

Cloud-based Services

Web Components A web application is hosted in a cloud platform for researchers to manage their image analytics projects and conduct experiments. The RISE analytical module includes the Image Analytic Workflow Management features, User Access Control functions, a Chatbot service, and the Feedback Command Interpreter that allows researchers to interact with the RISE web services. Researchers can also keep track of the progress of their experiments, check to see if any images have been produced by the SEM, preview the images that are already available, submit images for analysis, receive the results from the Image Processing Services, and save the images locally. The technologies used to build this service are *ReactJS* and *Vite* for the front-end development, *MongoDB* as the database management system, *Postman* for API testing and validation, and *Flask* and *Node.js* on the server side. Hosting for the server is provided by an *AWS EC2* instance, while image storage and retrieval are facilitated through an *AWS S3* bucket integrated into a cloudlet instance. Additional components on the face of the portal are a Dashboard tab that provides a preview of the number of images analyzed in the week; an Instruments tab (see Figure 3.4) that shows metadata of available instruments; a Storage tab that shows different types of storage available e.g., Relational database or cloud storage, and a Projects tab (see Figure 3.5) that shows the current projects, enhancing project management and collaboration. Additionally, the *Flask* application houses our Intelligent agent, which facilitates interaction with a Chatbot through RESTful APIs. An *x-auth-token header* is used to authenticate users against the web server.

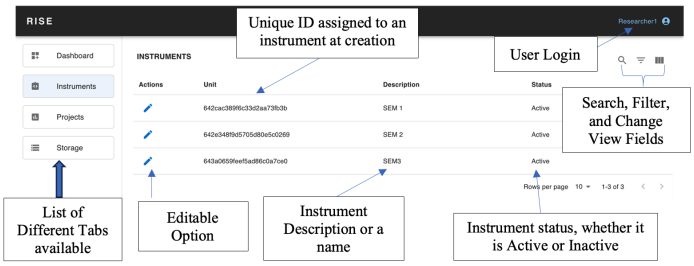


Figure 3.4: Screenshot of the Instruments tab enabled by the web services for displaying a selection of available instruments accessible to the logged-in user.

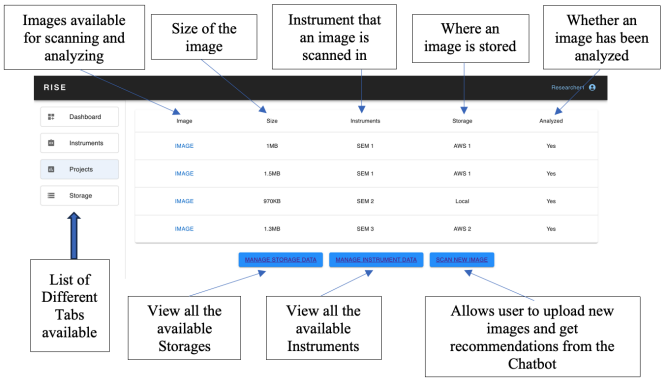


Figure 3.5: Screenshot of the Project tab in the portal, featuring comprehensive details of a chosen project. The web services showcase the project's associated images, accompanied by their respective metadata, including image name, size, storage location, SEM instrument used, and status of analysis completion.

Each project within the system maintains a collection of images that undergo scanning via the SEM. These SEM images exhibit distinct parameters, including resolution, volume image count, and precision, accompanied by associated metadata. At the backend, the web services are connected to the resource and service manager component where SEM resource management, SEM feedback generator, image analytics models, and Image storage management elements persist. Furthermore, on any specific project page, users are presented with additional options including the "Manage Storage Data" and "Manage Instrument Data" buttons, which provide users with insights into the current storage and instrument choices available for the respective project. Additionally, users are offered the "Scan New Image" button, which grants them access to a dedicated interface. Within this interface, users can upload images specific to the project, select an instrument, opt for a storage solution, and interact with a chatbot for further image refinement, as illustrated in Figure 3.6. The RISE agent allows users to improve the image quality based on the values suggested by our chatbot agent.

Informed by the results of previous experiment iterations and guided by the AI-based Feedback Commands Generator, the Chatbot service extends recommendations to researchers. In accordance with the image chosen by the researcher, the intelligent agent uses reinforcement learning (RL) [39] and provides recommendations for adjustments of SEM controller in terms of zoom, focus, and

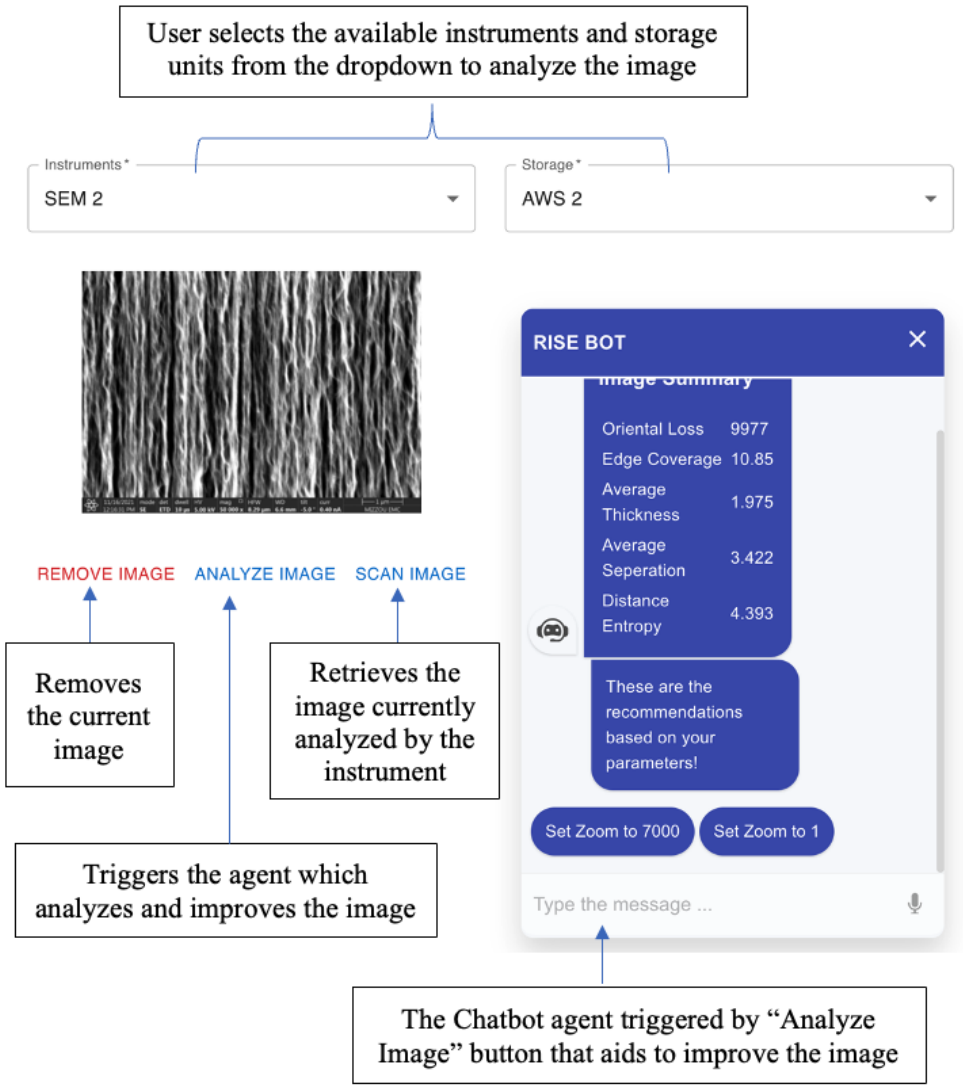


Figure 3.6: Screenshot showing the RL-based recommendations for the SEM Controller post-image analysis to optimize the parameters in image analysis.

contrast. These recommendations are based on the analysis of five critical image parameters: Oriental Loss, Distance Entropy, Average Thickness, Average Separation, and Edge Coverage. Subsequently, the researcher can accept or apply the suggested values, which are conveyed to the chatbot to interact with the corresponding APIs.

Specifically, upon the researcher's selection of the recommended options, the chatbot agent proceeds to generate a new image incorporating the specified zoom, focus, and contrast values as shown in Figure 3.7. If the researcher finds the resulting image satisfactory, they have the option to retain it. However, in cases where the user desires further adjustments, they can select the "generate new image" button. In response to this action, the agent resumes its operations in the background, producing new zoom, focus, and contrast values for the researcher's consideration. This iterative

process continues until the user is satisfied with the image quality.

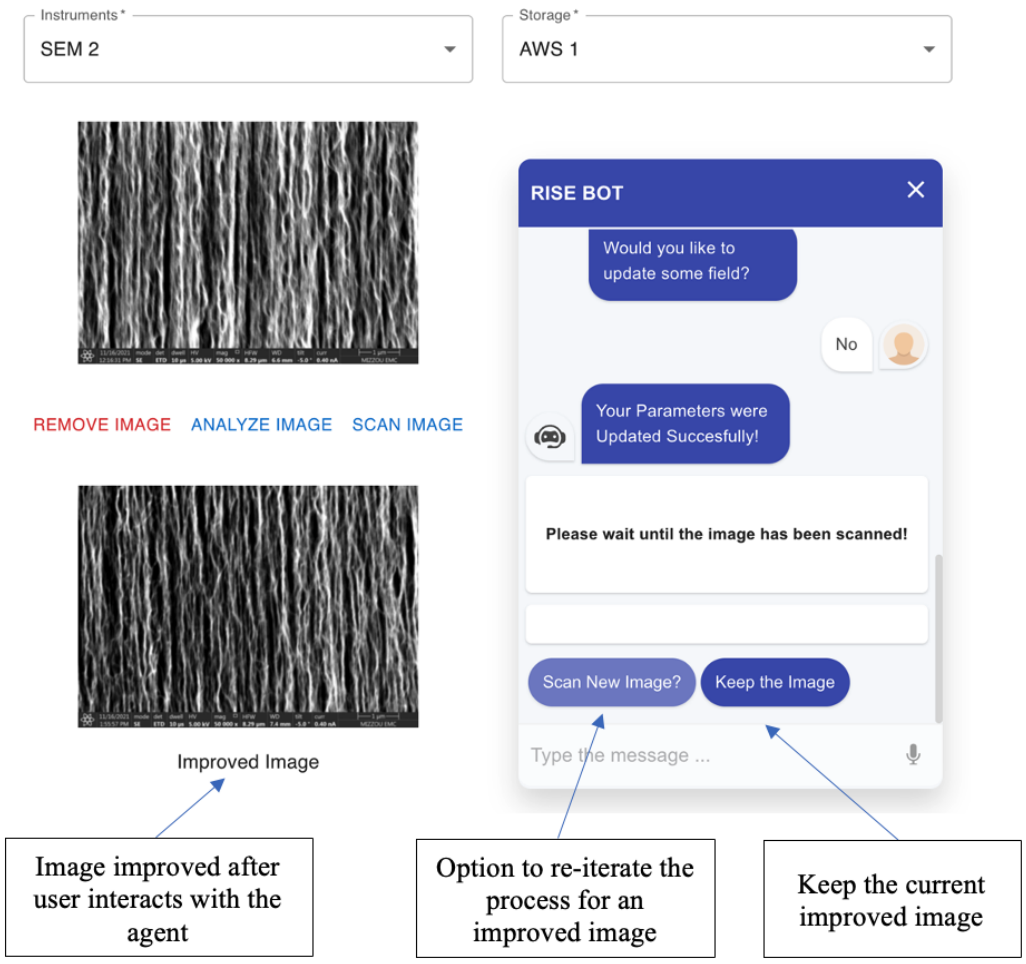


Figure 3.7: Screenshot showing enhanced image post-SEM parameter adjustments using parameters from the RL-based recommendations.

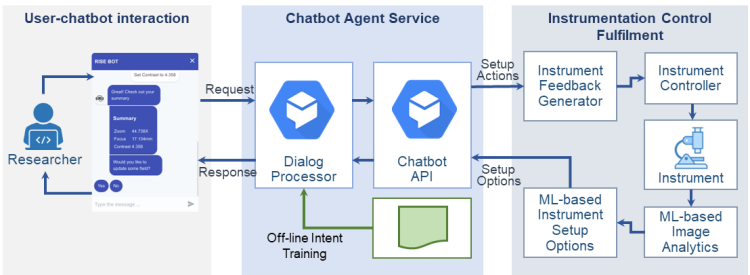


Figure 3.8: RISE Chatbot interaction for users to interact with APIs between the User and the Instrument positioned in the Instrumentation Control Fulfilment.

Resource and Service Manager

Our Resource and Service Manager comprises of the SEM resource management, SEM Feedback generator, Image Analytics Module and the Image Storage Management. These components are instrumental in streamlining the management of computational resources, storage solutions, and

associated services, ensuring efficient resource utilization. When the researcher chooses to analyze an image, it invokes the image analytics models at the back-end, where a deep learning algorithm [35] known as CNTSegNet is utilized. It is a novel dual loss, orientation-guided, self-supervised deep learning network specifically designed for CNT forest segmentation in SEM images. To evaluate the quality of CNT segmentation, five unsupervised measures are computed, namely orientation loss, edge coverage, average thickness, average separation, and distance entropy, whose sample values are listed in Table 3.1. These unsupervised segmentation evaluation measures play a crucial role in improving CNT forest segmentation results.

Table 3.1: Segmentation quality measures computed for a sample CNTSegNet segmentation output.

Measurement	Value
Orientation loss	9922
Edge coverage	15.64%
Average thickness	01.9965
Average separation	2.4233
Distance Entropy	4.1677

The Chatbot Agent shown in Figure 3.6 shows the image analysis summary, which includes the results of the five image segmentation parameters. Based on the results, it recommends improved SEM controller parameters such as new zoom, contrast, and focus using the module's SEM feedback generator element. The SEM feedback generator employs RL at the backend to improve the image. The new enhanced image is shown in Figure 3.7, which is obtained after modifying the SEM controller parameters based on the chatbot recommendations. On the other side, image storage management manages the image data as the name suggests. The user-selected image is sent from the storage cloudlet to the image analytic services for analysis, and the image metadata is simultaneously sent to the web service and stored in the image storage service.

SEM Local Lab Environment

By separating the SEM instrument from any external environment, a module hosted at the SEM's site safeguards it from any unauthorized access and related security issues. As a result, the SEM controller and the instrument cloudlet can coordinate for remote integration with the other RISE components. This module controls the Python Programmable Interface (PPI) API between the instrument cloudlet and the SEM controller via an SSH connection. When linked to the SEM Feedback Generator using a secure duplex connection, the HLL instrument REST API provides user commands to modify the SEM controller parameter for a new experiment. Additionally, it creates a simple channel of communication with the storage cloudlet of the image storage service component,

where it sends the SEM images for storage.

RISE Chatbot Assistance

The proposed Chatbot service serves as a communication channel within the RISE web services, facilitating vital user interactions during experiment feedback control. Its primary purpose is to foster conversational engagement between researchers and the RISE service functionality as illustrated in Figure 3.8. The Chatbot-Agent Service incorporates a Dialog Processor, a critical component responsible for handling user inquiries and formulating responses. To enhance its conversational abilities, the Dialog Processor leverages intent training, allowing it to understand and interpret user intents effectively. The Instrumentation Control Fulfilment module is integrated with the chatbot, facilitating instrumentation setup and control. This module collaborates closely with the Chatbot-Agent Service to ensure efficient execution of setup actions. This is again connected to a dynamic component that generates feedback commands for instrumentation control.

Image Storage Service

Similar to SEM Local Environment, the Image Storage Service Module is integrated to other components of the RISE via the Storage Cloudlet. It isolates and protects the stored data from any unauthorized access and associated security risks. The storage service and storage cloudlet are both connected via secured *SSH* connections, similar to the local SEM environment. Data Definition Language (DDL) and Data Manipulation Language (DML) commands are used for communication between the instrument cloudlet and the storage service. The storage cloudlet receives the SEM image from the instrument cloudlet and stores it in the SEM images repository. To store and send images, this module communicates with an image storage management that uses a secure connection.

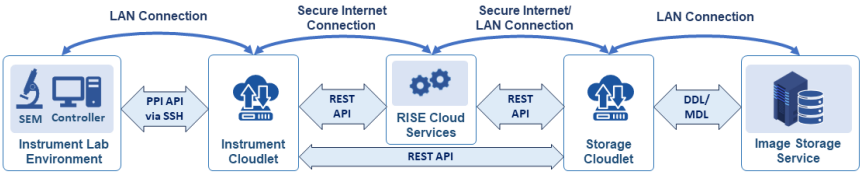


Figure 3.9: Illustration of steps involved in secure Cloudlet communications.

Security Components

Figure 3.9 illustrates the steps involved in the secure communication process between the cloudlets, a key aspect of the RISE web services security architecture. Our goal in the design of the security mechanisms within our RISE web services is to guarantee the confidentiality, integrity, and availability

of both data and instrumentation resources. To safeguard data and maintain system integrity, the RISE uses session-based authentication, which is strengthened by the use of unique session IDs. Features such as session timeouts, IP tracking, and protection against Cross-Site Request Forgery (CSRF) attacks are incorporated. Furthermore, the RISE architecture utilizes REST APIs and PPI APIs and a High-Level Language (HLL), with security enforced via the Advanced Encryption Standard (AES) and secure SSH connections. The instrument cloudlet securely converts user requests to original PPI commands and communicates with the SEM controller through SSH over a LAN Connection. SEM controller responds to the cloudlet, which sends data back to the portal via REST API over a Secure Internet Connection. Image data is directly sent from the instrument to the storage cloudlet using Secure Internet or LAN Connection for Image storage Service. Storage Cloudlet and Image Storage Service can communicate using DDL/DML commands over LAN Connection. To ensure secure image data transfer and storage, the RISE maintains encrypted communication channels and employs dedicated ports.

The authentication mechanisms employed are essential to verify the identity of users or entities accessing a system, ensuring access control to sensitive data and resources while mitigating data breaches and security risks. The work in [40] explained various authentication methods, including Password-based, Multi-Factor (MFA), Certificate-based, Biometric, Session-based, and Token-based authentication. In our web services, Session-based authentication and authorization are employed, that generates unique session IDs for authenticated users. The session IDs are stored on the server side, facilitating continued authentication and access to protected resources. This approach incorporates security features such as session timeouts, IP tracking, and anti-CSRF protection.

Resource protection mechanisms are also incorporated in our RISE web services.In our work, all data shared through APIs is encrypted to ensure confidentiality and privacy. The Cypher class of the *node.js crypto module* supports AES-128, AES-192, and AES-256 encryption. The *createCipheriv()* method with algorithm, security key, and random bytes as options to encrypt the data into ciphertext using base64 encoding are employed to complete the process with the *final()* method. For decryption, similar steps are followed using the same parameters and the *createDecipheriv()* method to unlock the data.

Referring to Figure 3.9, our method aligns with the principles outlined in [41], which introduces a 'Reference Roadmap' for ensuring reliability and high availability in cloud computing environments. This roadmap is divided into four key steps, addressing questions related to 'Where?', 'Which?', 'When?', and 'How?'. Our approach leverages encrypted high-level commands to establish secure API connections between the web service and a Cloudlet, ensuring data privacy and integrity. The

Cloudlet, based on request data, decrypts these commands, generating real/low-level commands. In a private network configuration, the Instrument Cloudlet forms a secure SSH connection to the SEM controller, as depicted in Figure 3.9. Simultaneously, the Storage Cloudlet connects securely to private network storage, ensuring that original commands do not traverse the public network. This strategic configuration enhances system integrity, data accuracy, and availability, safeguarding these aspects exclusively for authorized users.

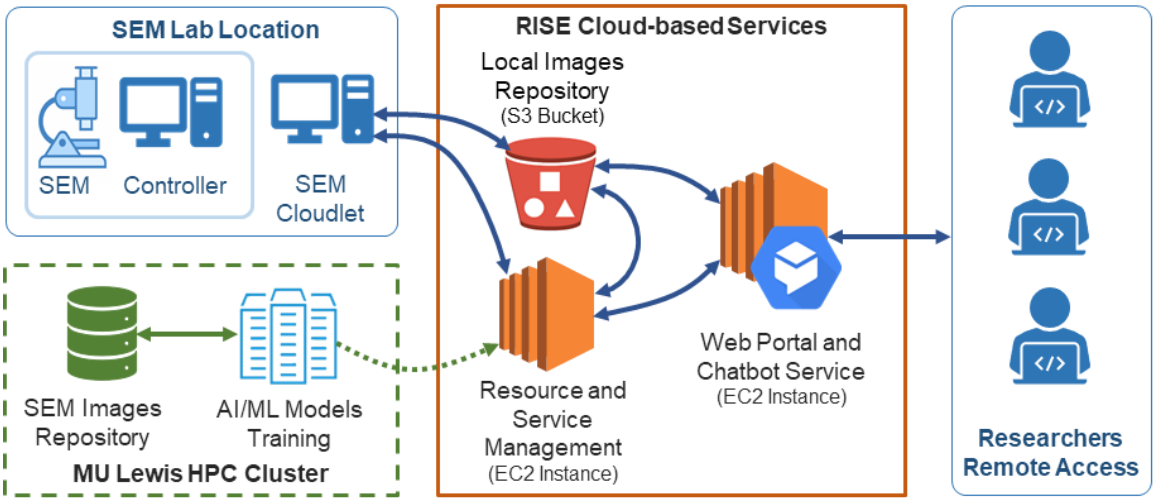


Figure 3.10: RISE testbed infrastructure showing the remote lab location of the SEM, related controller, and Cloudlet with Internet access; the off-line AI/ML training environment hosted by the MU Lewis HP Cluster; the cloud-based RISE services including a host for the ML analytic models, local image repository, and host for the web service and chatbot service.

3.1.4 Performance Evaluation

In this section, the implementation and evaluation of our RISE environment is detailed begining with describing our testbed implementation, followed by an overview of our SEM CNT image dataset. Subsequently, a performance comparison of RL/IL agent-based instrument control approaches for selecting SEM parameters to guide the CNT image analytics process is conducted.

RISE Web Services Testbed Implementation

Figure 3.10 illustrates the cloud infrastructure implementing the RISE testbed, where the RISE environment is implemented and evaluated. This infrastructure integrates all system components within a cloud-based platform, including the Phenom SEM, the MU Lewis HPC center (utilized for training AI-ML based models), and RISE cloud-based services deployed on AWS. Additionally, the web interface enables users to access the system remotely from diverse locations.

The SEM instrument communicates with the cloud-hosted RISE web services through the SEM Cloudlet, acting as an intermediary. It translates commands between RISE web services and the SEM instrument using (High Level Language) HLL commands to configure instruments and collect scanned images. Images are transmitted via a REST API to an *AWS S3* bucket, serving as the cloud-based image repository. The image storage is streamlined by implementing an interface in our image storage cloudlet, optimizing storage and retrieval. The CNTSEgNet [35] model was developed and trained at the MU Lewis HPC cluster. Training CNT images are stored locally at the HPC facility. After training, the model is transferred to a cloud-based compute instance for assembling CNT segmentation analysis. The RL/IL-based SEM feedback control agent are trained in a local machine and then transferred to the testbed to analyze the five resultant parameters from the CNT segmentation model and generate the most suitable values for zoom, focus, and contrast to set the SEM configuration to improve the quality of the image on a next iteration of the experiment.

The RISE web services run on two *AWS EC2* virtual machine instances. The first instance hosts the ML models to analyze new CNT images from the S3 image repository by performing segmentation using CNTSegNet. It also hosts the RL and IL agents that generates suggestions for the zoom, focus, and contrast settings to enhance image scan quality. The second *AWS EC2* instance hosts the web service and chatbot services. They provide the interface for researchers to define SEM parameters for zoom, focus, and contrast with the aid of the chatbot. Researchers can then confirm the final settings to assemble the feedback SEM commands to be sent to the instrument via a REST API. Upon completion, the new scanned CNT image is stored in the *AWS S3* bucket, triggering notifications to the web services. Researchers can review the images and iterate with the chatbot assistant to steer new adjustments on the SEM as needed.

SEM CNT Images Data Set

To conduct offline training for our RL and IL agents, actual CNT images from the SEM are gathered, ensuring they met the required quality standards. This dataset comprises of images with three different Zoom magnification levels (25000, 50000, 100000), Focus values ranging from 5.8 to 8.9 mm, and Contrast values ranging from 58.5 to 72.9. The test dataset comprises 48 samples, with 20 from a Zoom of 25000, 20 from a Zoom of 50000, and 8 from a Zoom of 100000. This intentional uneven distribution ensures an optimal training-to-testing data ratio for each Zoom category. Through CNT segmentation, five evaluation metrics (Orientation Loss, Edge Coverage, Average Thickness, Average Separation, and Distance Entropy) are derived. Utilizing these segmentation metrics results, RL and IL agents are trained to predict three SEM setup parameters (Zoom, Focus, Contrast) with the aim

of scanning CNT images comparable in quality to the original ones. The CNT dataset is publicly accessible at [42].

The test dataset comprises 48 samples, with 20 from a Zoom of 25000, 20 from a Zoom of 50000, and 8 from a Zoom of 100000. This intentional uneven distribution ensures an optimal training-to-testing data ratio for each Zoom category. Through CNT segmentation, five evaluation metrics (Orientation Loss, Edge Coverage, Average Thickness, Average Separation, and Distance Entropy) are derived. Utilizing these segmentation metrics results, our RL and IL agents are trained to predict three SEM setup parameters (Zoom, Focus, Contrast) with the aim of scanning CNT images comparable in quality to the original ones. The CNT dataset is publicly accessible at [42].

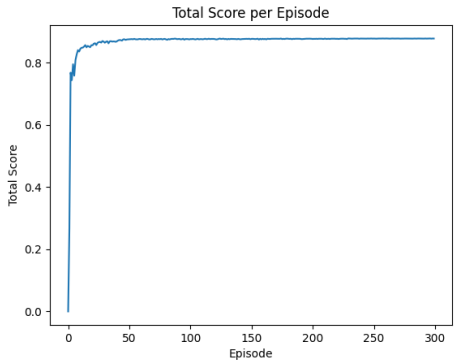
3.1.5 Results of CNT Image Segmentation and Characterization Experiments

This subsection presents the experimental findings derived from the implementation of the CNT image segmentation and characterization looking to determine the zoom focus and contrast of the CNT image.

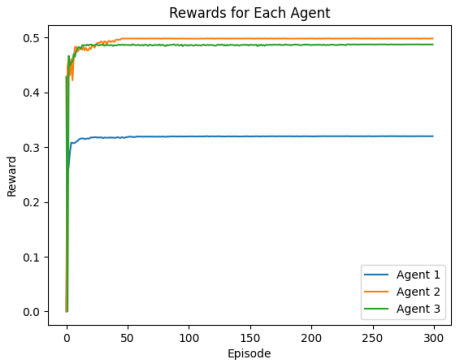
RL-based Image Characterization Results

With MADDPG, by understanding the correlations between the 3 agents and the 5 image parameters, the model provided learning rate over iterations as observed in the image 3.11a. This suggests that the RL agents learned effective policies to maximize correlations between scanning parameters and image parameters. This indicates the system can automatically find the configuration that produces the best possible SEM images. The Hyperparameter settings for the policy are provided in the Table 3.2. The reward function was defined to incentivize the agents to select actions that will result in higher correlations. Our experiments with MADDPG demonstrated its effectiveness in achieving the desired correlations between scanning parameters and image parameters in the context of SEM image acquisition. The agents were able to learn effective policies through trial and error, maximizing their cumulative rewards over time. The reward of each agent accumulated over training can be visualized in the image 3.11b.

Using our CNT data set, a customized image environment designed for our RL tasks is implemented. This environment features a multi-dimensional state space (see **Algorithm 1)**, capturing key image quality metrics such as Orientation Loss, Edge Coverage, Average Thickness, Average Separation, and Distance Entropy. These metrics emulate the settings of a SEM, with actions corresponding to adjustments in Zoom, Focus, and Contrast levels. To ensure meaningful training, a reward structure



(a) Total rewards for the MADDPG model over the training over 3000 epochs and hyperparameters referred in Table 3.2



(b) Rewards for each agent over the training episodes based on how close the correlations are to the actual values

Figure 3.11: Training results of the MADDPG model.

Hyperparameter	Value
Alpha	0.001
Beta	0.001
Buffer Size	1000000
Gamma	0.95
Tau	0.01

Table 3.2: Hyperparameters used in **Algorithm 1** to tune and recommend suitable parameters.

that incentivizes SEM settings leading to target image quality is established that is defined by specific thresholds for each metric. Simultaneously, actions outside the permissible range incur penalties. Throughout training, the environment tracks both state and action histories, facilitating subsequent analysis.

Challenges on training the RL and IL models

Significant results are achieved using RL and IL approaches to determine zoom, focus, and contrast parameters by analyzing CNT image segmentation metrics. However, these approaches posed several challenges, especially given our limited dataset. One major issue was the disparity in effectiveness across different parameters. This highlights the difficulty of fine-tuning RL and IL models with limited and imbalanced data. The IL-based model outperformed the RL-based model by directly predicting the image scanning parameters. In contrast, our RL implementation requires translating predicted image segmentation into correlations with image scanning parameters, which complicates the task. The RL model, specifically using MADDPG, faced challenges in predicting image scanning parameters due to its sensitivity to input variability. In dynamic environments like SEM image acquisition, changes in conditions can affect correlations between zoom, focus, and contrast, leading

to suboptimal adjustments and unstable performance. Despite its relative success, the IL-based approach also had limitations, particularly with Contrast, due to the complexity of learning from expert demonstrations with limited data. Data augmentation, while helpful, cannot fully compensate for the lack of diverse real-world data, crucial for robust training. The limited dataset restricts the models' ability to learn comprehensive patterns, requiring extensive preprocessing and augmentation, which may still fall short in replicating the variability of larger datasets.

3.1.6 Conclusion and Future Work

In this thesis, a novel suite of RISE web services for automated image analytics is presented, enabling feedback control of remote instrumentation in discovery processes, such as in material science. Our approach successfully addresses performance improvement and data/instruments security during image analytics tasks, providing seamless and secure communication for remote access to scientific instruments. This implements and compares RL and IL agent-based approaches to identify the optimal learning method for guiding real-time image processing tasks during in-situ CNT manufacturing on cyber-enabled SEM instruments.

The RL-based approach, utilizing the MADDPG algorithm, relies on correlations between the five segmentation parameters and the CNT image scanning parameters (i.e., zoom, focus, contrast) to predict recommendations for the SEM to capture quality images during scanning. However, translating these predicted correlations back to actual CNT image scanning parameter values requires additional effort. In contrast, the IL-based approach employs a functional-gradient method to mimic expert actions, providing direct recommendations for SEM setup parameters. These findings highlight the effectiveness of IL over RL in improving CNT image collection. This direct output sets it apart from our RL method in a beneficial manner. The RL and IL agents are seamlessly integrated into the RISE solution, facilitating user-AI agent interactions through chatbot-based services. This integration enables users to directly engage with cyber-enabled instruments using RL and IL agents, streamlining manual CNT manufacturing processes.

Future work could involve providing iterative feedback control to predict and recommend parameters for improving the quality of CNT images based on the characterization of ideal CNT image parameters. Additionally, expanding the RISE system with web services that integrate our RL/IL algorithms for a broader range of image analytics applications and CNT synthesis control is a promising direction. This expansion could involve controlling the CNT growth rate based on current growth rate and SEM chamber conditions, such as temperature and pressure.

3.2 CyEscape: Introduction

The escalating prevalence of cyber attacks underscores the critical need for comprehensive cybersecurity education [43]. Traditional methods often lack the practical, hands-on training necessary to effectively counter these threats, necessitating innovative approaches that combine theoretical knowledge with practical skills [44]. The rapid advancement of Virtual Reality (VR) technology presents a transformative opportunity. Virtual Reality Learning Environments (VRLEs) have the capacity to deliver immersive and engaging experiences, thereby serving as a potent platform to effectively address the challenges of cybersecurity education. However, achieving this level of engagement requires meticulous design tailored to the needs and preferences of the end user. Researchers have highlighted the potential of game-based learning in VR environments to simulate cyber threats and facilitate experiential learning, as seen in [11], [12], and [45]. By leveraging VRLEs, there is a potential to create dynamic and interactive learning environments where students can navigate simulated cyber incidents, develop practical skills, and retain knowledge.

This section of thesis presents a novel framework viz., "CyEscape" to explore the potential by combining the power of VRLEs with cybersecurity education. CyEscape offers escape rooms set in VR environments, where learners navigate real-world cybersecurity incidents guided by pedagogical agents driven by reinforcement learning (RL) [46], and overcome attack impacts using active defense techniques [47]. The framework components shown in Figure 3.12 ensure personalized feedback and adaptive game-based learning experiences for students, fostering a deeper understanding of cybersecurity concepts and skills. Utilizing user progress monitoring and state-of-the-art technologies such as OpenAI [48] to develop the conversation aspects of the pedagogical agent, CyEscape advances cybersecurity education by fostering immersive, interactive, and effective learning.

Despite the potential benefits, integrating advanced technologies such as RL-powered pedagogical agents into VRLEs poses several challenges. While AI technologies such as OpenAI's ChatGPT [48] offer ways to create pedagogical agents, there is a knowledge gap regarding how to effectively integrate such agents into VR environments for cybersecurity education [26],[23]. Moreover, responses from AI-based chatbots can be vague or broad to provide meaningful guidance in complex cyber attack incident scenarios, highlighting the need for targeted learning algorithms that drive the pedagogical agents.

CyEscape addresses these challenges by simulating real-world cyber attack incidents within immersive VR environments, offering learners practical hands-on experience in cyber defense. The

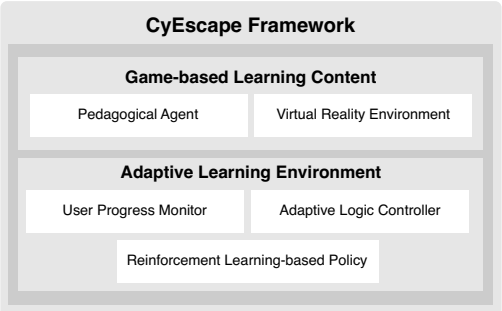


Figure 3.12: Overview of CyEscape framework that enables cybersecurity training to improve learner knowledge and hands-on skills.

inclusion of a pedagogical agent that uses RL enhances the learning process, providing personalized guidance and feedback as students navigate through various cyber defense learning exercises. Utilizing MetaQuest 2, [49], and assets from the Unity Asset Store, [50], a comprehensive curriculum comprising of game-based learning exercises to defend against different types of cyber attacks (e.g., Distributed Denial of Service, Sniffing, Advanced Persistent Threats) is developed.

Our evaluation experiments first aim to rigorously assess the performance of our RL algorithm by showcasing its efficacy in enhancing the utility of our pedagogical agent. Additionally, comprehensive usability studies to evaluate the user-friendliness and practical usability of the CyEscape VRLE from the participants' perspective is conducted. These studies provide valuable insights into the usability of the CyEscape implementation, particularly focusing on its effectiveness in engaging diverse students and enhancing their cybersecurity knowledge and skills through cyber attack-themed escape rooms.

The remainder of this thesis is organized as follows: Section 3.2.1 outlines the motivation behind our CyEscape framework design, and the challenges that are to be addressed. Section 3.2.2 delves into our solution approach, detailing the CyEscape components implemented, including the pedagogical agent and the cyber defense curriculum design. Section 3.2.4 presents the performance evaluation results of our RL approach and the findings from usability studies. Section 3.2.5 concludes the thesis.

3.2.1 Problem Background and Challenges

Cybersecurity VRLEs

In traditional cybersecurity education, students often face limitations in acquiring practical skills and real-world experience due to reliance on theoretical lectures and static materials [44]. This approach is inadequate in preparing learners to effectively combat the rapidly evolving and advanced cyber

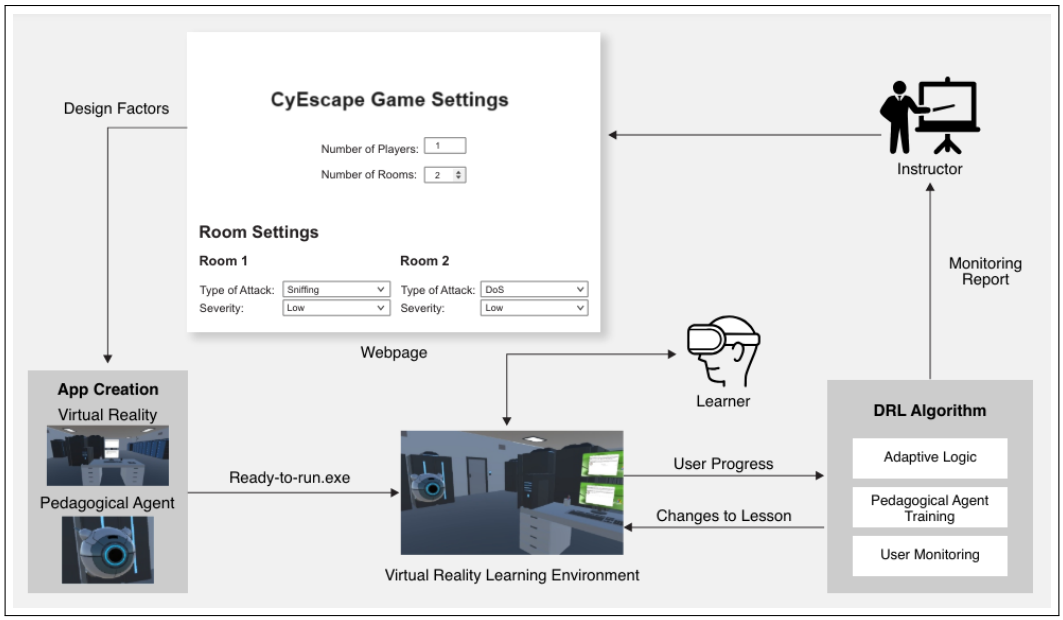


Figure 3.13: System Architecture of a CyEscape enabled adaptive VRLE to teach cybersecurity knowledge and skills leveraging an RL-based PA.

threats of today's digital landscape [43]. Recognizing these deficiencies, there is a growing demand for innovative educational methodologies that can provide hands-on training and immersive learning experiences.

VRLEs offer a promising solution by providing dynamic and interactive platforms where learners can engage with realistic simulations of cyber incidents [22, 51]. By immersing students in virtual environments, VRLEs enable them to experiment with various strategies, respond to simulated attacks, and receive immediate feedback on their actions [22]. This experiential learning approach not only enhances comprehension but also cultivates critical thinking and problem-solving skills essential for cybersecurity professionals [51]. The challenge in CyEscape is to create VRLEs that can provide immersive learning experiences tailored to cybersecurity training, addressing deficiencies in traditional methods. Another signficant challenge for CyEscape is to simulate real-world cyber incidents, and fosters critical thinking and rapid decision-making under pressure, bridging the gap between theory and practice.

Cybersecurity Escape Rooms

Escape rooms immerse participants in realistic scenarios, challenging them to thwart cyber attacks within a set timeframe [15]. This hands-on approach fosters critical thinking and collaboration, reflecting real-world cybersecurity incidents. In cybersecurity education, they serve as simulated

environments where learners translate theoretical knowledge into practical application [52].

In a cybersecurity Escape Room VRLE, participants can engage in simulated cyber attack scenarios, starting with system health checks to detect suspicious activities. Tasks can involve analyzing IP address patterns, investigating attacker traffic, and implementing defensive measures like blacklisting attackers and cleaning up file systems. This immersive learning equips participants with practical cybersecurity skills and incident response techniques, preparing them to detect, defend against, and mitigate cyber threats in professional settings [53].

Consequently, another challenge for CyEscape is to gamify the learning process via use of virtual escape rooms, where participants learn by identifying vulnerabilities, analyzing attack vectors, and deploying effective defense strategies, promoting collaboration in addressing cyber threats [16].

Pedagogical Agent Integration

Achieving personalized learning within a virtual environment necessitates the integration of adaptive instructional strategies and dynamic content delivery mechanisms. By creating immersive environments that faithfully simulate real-world cyber attack incident scenarios, learners can be made to remain consistently engaged. This entails striking a delicate balance between realism and interactivity, as the VRLE must present scenarios such as data breaches and phishing attacks in a manner that captivates learners without overwhelming them.

For the above purpose, the integration of an intelligent PA can help guide the learning of the students, and tailor the VRLE experience to accommodate the diverse learning paces, styles, and preferences of individual students, [24] and [25]. Integrating cutting-edge technologies such as OpenAI, [48], and RL algorithms, [54], can support such features of a PA in the VRLE. Thus, the challenge for CyEscape is to leverage an intelligent PA approach capable of effectively guiding learners through the escape room based VRLEs and provide personalized guidance and feedback. The PA should interact with the learners with user-friendly voice/text interfaces and guide the progress of the learning exercises for a range of learners spanning novice to advanced levels, as well as learns with diverse backgrounds and learning abilities/styles.

3.2.2 CyEscape Solution Design

This section outlines the system architecture of CyEscape and focus on three key aspects: Design of the Content, Design of the PA, and Design of the UI.

System Architecture

The system architecture of CyEscape, as illustrated in Figure 3.13, is designed to provide a flexible framework for delivering immersive cybersecurity training experiences to diverse learners. It comprises of several components, including the VR environment, the backend infrastructure for data management and analytics, and the frontend application for user interaction. The VR environment is built with Unity 2022.3.9f1, leveraging assets from the Unity Asset Store, including Meta XR All-in-one SDK [55] and OpenAI Plugin for Unity [56] to create realistic scenarios of cyber attack incidents. The backend infrastructure utilizes cloud-based services for storing user data, managing session states, and generating analytics reports. The frontend application provides an intuitive interface for users to navigate the VR environment, interact with the PA, and track their learning progress.

Table 3.3: Escape Room design to implement various cyber attack incidents in the learning content of CyEscape.

lXXX

Attacks/ Severity	**Easy**	**Medium**	**Tough**
Sniffing	Identify and locate basic packet sniffing tools within the network.	Analyze captured packets to identify sensitive information such as usernames and passwords.	Implement countermeasures to prevent packet sniffing attacks and secure the network.
DoS	Recognize signs of a denial of service (DoS) attack, such as unusually high traffic or unresponsive services.	Mitigate a simple DoS attack by implementing basic filtering rules or rate-limiting techniques.	Defend against more advanced DoS attacks by deploying advanced mitigation strategies such as moving target defense.
APM	Identify suspicious network traffic patterns indicative of advanced persistent mining (APM) activities.	Utilize intrusion detection systems (IDS) to detect APM activities.	Implement proactive measures to prevent and disrupt ongoing APM activities.
APT	Recognize initial signs of advanced persistent threat (APT) presence.	Conduct forensic analysis to trace the origins and techniques employed by APT actors.	Develop and implement a comprehensive incident response plan to contain and eradicate APT presence while minimizing damage and restoring operations.

Design of the Content CyEscape employs content design to offer immersive and effective learning experiences. In CyEscape, learners engage in hands-on exercises within a simulated cyber environment within escape rooms with various cyber attack incidents. The design of content within CyEscape features realistic cyber attack incident scenarios as shown in Table 3.3. In the following, the CyEscape's content design is described, highlighting the pivotal roles of instructor input via the UI and the RL algorithm used by the PA in shaping the learning experience.

Escape Room Design

CyEscape showcases its utilization of VR technology to simulate cyber attacks within an immersive

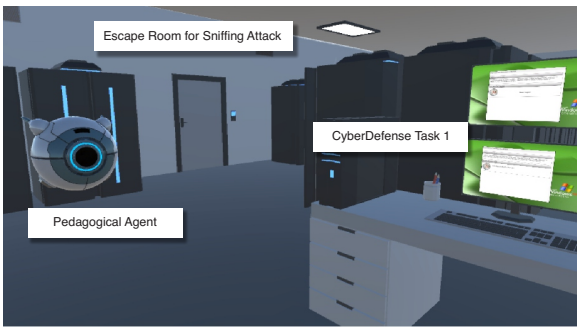


Figure 3.14: Screenshot of the Escape Room customized for the learner to interact with the Pedagogical Agent guiding a learning task on defending the VR assets against a sniffing attack.

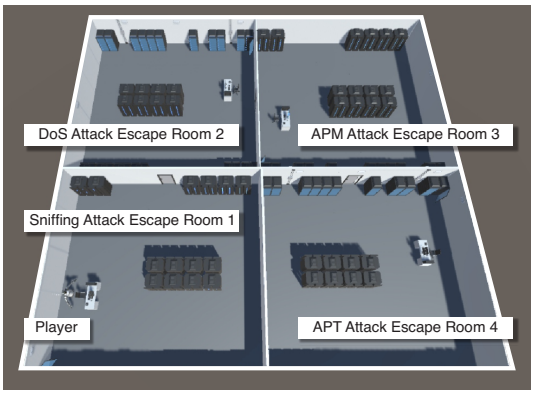


Figure 3.15: Four rooms created based on user input, which includes number of rooms, number of users, types of attacks and level of difficulty.

environment, with PA communication informing users of the type of attack, as seen in Figure 3.14. Each room within CyEscape presents a series of challenges and mini-games representing different aspects of a cyber attack, facilitating hands-on learning in a controlled, realistic setting. For instance, in a simulated sniffing attack, users must complete three separate challenges, each demonstrating a step in mitigating threats within a system. Throughout these challenges, the PA provides guidance and explanations, enhancing the learning process in an engaging manner.

UI for Instructor Input

Instructors play a central role in shaping the learning environment by providing input via the UI, guiding the creation of the VR environment and the development of the PA. Key parameters such as the number of rooms, users, types of attacks, and desired difficulty levels are inputted through the UI, shaping the overall structure and parameters of the VR rooms featuring the PA as shown in Figure 3.14.

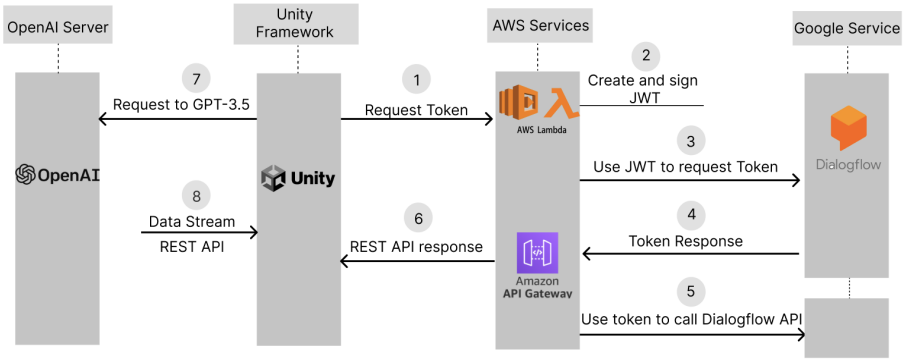


Figure 3.16: API communication between Dialogflow, OpenAI and Unity enabling users to interact with the PA to learn cybersecurity skills.

RL Agent

The RL agent features an algorithm that enhances the adaptability of the learning experience by analyzing user progress within the VR environment and suggesting adjustments to upcoming tasks in which the PA is involved with learner interactions. Performance metrics such as time-on-task and task difficulty inform the algorithm's dynamic adjustment of task difficulty, ensuring an optimized learning trajectory tailored to individual learners.

Pedagogical Agent Implementation

The PA implementation is focused on communications with the learners in the escape rooms, guiding them through immersive learning experiences on mitigating impact of cyber attack incidents. An API interfaces is developed for the orchestration of the various PA components in order to facilitate effective dialogue and learner support. An RL algorithm within the PA, enabling dynamic adaptation to user actions and environmental cues is also implemented. In the following, details of the API and RL algorithm are presented to enhance user engagement and foster effective learning outcomes.

PA Communication Infrastructure In CyEscape, the PA serves as a central component in CyEscape's immersive learning environment, orchestrating interactions between learners and the VR environment. The PA's architecture, depicted in Figure 3.16, integrates Unity, Google Dialogflow, AWS resources, and OpenAI technologies to create a seamless learning experience. Within the Unity framework, users engage with the PA in gamified scenarios that enhance their understanding of cybersecurity concepts while completing learning tasks in escape rooms.

Through API communication, the PA leverages Dialogflow to understand and respond to user queries, providing dynamic interactions tailored to individual learning needs [57]. AWS Lambda

automates the generation of access tokens, ensuring continuous access to protected resources without disrupting user sessions. Additionally, ChatGPT enables the PA to address generic queries related to cyber attacks and mitigation techniques, while Whisper facilitates multilingual communication, expanding the accessibility of the learning experience [48]. For the PA to seamlessly integrate speech input and response conversion, Amazon Polly [58] is leveraged.

Relying on Deep RL methods such as DQN, the PA adapts its guidance strategies based on user interactions, offering personalized learning experiences tailored to individual progress and performance. By combining rule-based heuristics with machine learning algorithms, the PA provides contextualized support, guiding users through defensive actions against cyber attacks presented in escape rooms. This approach enhances engagement and ensures targeted instruction and support for users with diverse profiles, including those with neurodivergent needs.

RL enabling adaptive difficulty

To dynamically adjust the level of difficulty based on the time a user takes to complete a task, a reinforcement learning (RL) agent utilizing Q-Learning is employed. The agent's primary objective is to adapt to the user's pace in completing tasks, thereby enhancing their overall gaming experience. If the user completes the task within a predefined threshold time, the difficulty of the subsequent task increases significantly; otherwise, the difficulty decreases, ensuring a balanced experience.

Algorithm 2: Q-Learning for adaptive difficulty

Require: difficulty: current difficulty setting the player is in and success: whether the user has successfully finished a task.
Ensure: q_table: initialized with number of states as rows and actions as columns

initialize $\alpha, \gamma and \epsilon$
for each episode in range(num_episodes) **do**
  Reset state
  while the next difficulty is not chosen **do**
    $\text{action} = \begin{cases} \text{take a random action, if random(0,1) ¡ epsilon} \\ \max\{q\_table(\text{state})\}, \text{otherwise} \end{cases}$
    q_value = q_table[state, action]
    next_value = max(q_table[state])
    $new\_value = (1 - \alpha) * q\_value + \alpha * (\text{reward} + \gamma * next\_value)$
  end while
end for

The algorithm 2 outlines the Q-Learning algorithm that is leveraged to achieve adaptive difficulty. After each task, the agent collects the current difficulty and whether or not the user has succeeded. The q-table created from the algorithm returns the next difficulty level. The state space, action space for the algorithm are defined as:

State Space: The state space in the CyberDefense environment is represented as a discrete set of states, specifically defined by the task's current level of difficulty. In this environment, there are three possible levels of difficulty (0, 1, and 2), thus resulting in a discrete state space with three states.

$$\mathcal{S} = \{0, 1, 2, ..., |difficulty\_levels|\}$$

Action Space: The action space consists of discrete actions that an agent can take. There are three possible actions the agent can choose from, each corresponding to a specific maneuver to counter the cyber threat at the current level of difficulty.

$$\mathcal{A} = \{0, 1, 2, ..., |level\_chosen|\}$$

This environment is positively rewarded dynamically every-time the agent chooses the correct difficulty level and penalized otherwise. The agent then iteratively interacts with the environment and he Q-table is then constructed with the Bellman's equation:

$$Q(s, a)^* \leftarrow Q(s, a) + \alpha[r + \gamma max(Q(s^1, a^1)) - Q(s, a)] \quad (3.1)$$

This algorithm is hosted in a Flask server. Every-time a task is completed, a C# script invokes this Flask server. This collects the next difficulty setting and suggests it for the next level.

RL enabling Role of an Instructor

To aid users in defending against simulated cyber attacks, CyEscape leverages a DQN-based RL algorithm in the role of an instructor. Similar to human instructors, the RL agent dynamically adjusts defense strategies to counter ongoing threats effectively. It provides context-aware recommendations tailored to specific attack scenarios encountered by users. Algorithm 3 outlines the training process using DQN with experience replay. Our environment simulates a multi-level setting where the agent encounters various cyber attacks, each represented by a distinct state. At each level, the agent must select specific actions, corresponding to mitigation strategies, to counteract the ongoing cyber attack effectively. The environment provides rewards based on the effectiveness of the chosen action and penalizes the agent for incorrect actions. The state, action, and reward spaces are defined as follows

State Space: The state represents the current cyber attack scenario the agent is facing. Let $\mathcal{S}$ be the set of possible states, where each state $s \in \mathcal{S}$ represents a different attack scenario based on

the current level and the number of possible attacks in the level:

$$\mathcal{S} = \{0, 1, 2, ..., |attacks\_possible|\}$$

Action Space: In our scenario, actions correspond to mitigation strategies recommended by the RL-agent to counteract the ongoing cyber attack. Each action corresponds to a specific approach the agent can recommend the user to protect the system at the level. The action space $\mathcal{A}$ is a set of individual actions a, where a represents the 'recommended prevention' attribute of our environment, mapping to relevant mitigation techniques:

$$\mathcal{A} = \{0, 1, 2, ..., |recommend\_prevention|\}$$

Transition Dynamics: The transition dynamics of the environment account for level progression rewards and termination conditions based on task completion. When all tasks in the current level are complete, the agent advances to the next level. The transition dynamics can be defined as:

$$s' \sim P(\text{next state}|s, a)$$

Reward: The reward function $R(s, a)$ represents the immediate reward obtained when the agent takes action a in state s. Successfully recommending the corresponding mitigation technique and completing a level accumulates positive rewards, while inaction or user delay attracts negative rewards. The reward function is defined as $R : \mathcal{S} \times \mathcal{A} \to \mathbb{R}$. The agent's goal is to learn a policy $\pi : \mathcal{S} \to \mathcal{A}$ that maximizes the expected cumulative reward over time.

By iteratively learning and adapting its guidance, the algorithm guides the users through different challenges while ensuring users receive timely and effective support throughout their learning journey.

3.2.3 Exemplar Sniffing Escape Room Scenario

This section delves into an exemplar escape room scenario within CyEscape, focusing on the Sniffing concept. The related immersive experience showcases the dynamic and adaptive nature of our PA-guided escape rooms for cybersecurity education.

The Sniffing escape room within CyEscape serves as a simulated environment where learners engage in a series of tasks designed to simulate the detection and mitigation of a sniffing attack. The room incorporates gamified elements and real-time feedback to enhance learner engagement and

Algorithm 3: Deep Q-Network with experience replay

Initialize replay memory to fit the model
Initialize a random action based on level
For each episode in range(num_episodes):
    Reset state & observation and reshape state size
    For each time in range(num_epochs):
        Append state, observation, reward(R), done flag to memory
        If random $\leq \epsilon$:
            Return random action
        Else:
            $q\_values \leftarrow$ predict state from the model
            Return max q_values
        State $\leftarrow$ next_state
        If done $\leftarrow$ True: Break
If agent memory exceeds buffer:

$$\text{target} = \begin{cases} \mathrm{R} + \gamma \cdot \max(\text{model.predict(next\_state)}[0]), \text{ if not done} \\ \\ \mathrm{R}, \text{ otherwise} \end{cases}$$

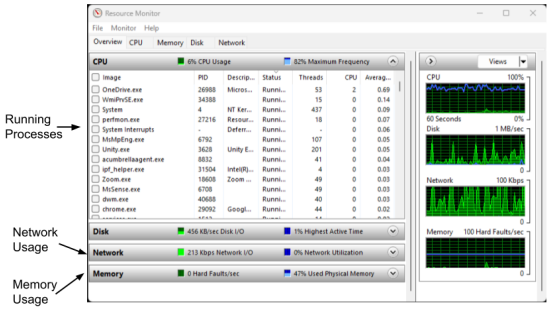


Figure 3.17: Simulated tool in the VRLE that leads the participants in running a system health check to look for any suspicious activities on the network or file systems.

effectiveness, as listed below:

Detection of Suspicious Activities: Upon entering the room, learners are tasked with running a system health check, seen in Figure 3.17, to identify any suspicious activities on the network or file system. Real-time feedback mechanisms, such as siren lights and icons indicating urgency, alert learners to the presence of a sniffing attack in progress.

Identifying Anomalies in IP Addresses: Learners engage in a game-like activity to identify abnormality in a list of IP addresses, mimicking the process of detecting anomalous network traffic associated with a sniffing attack. Upon successful identification, learners proceed to blacklist the attacker, simulating proactive threat mitigation measures. Snippets of this game are seen in Figures 3.18 and 3.19.

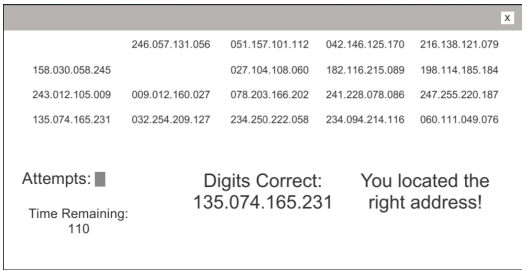


Figure 3.18: The screen seen when the Attacker has been found.

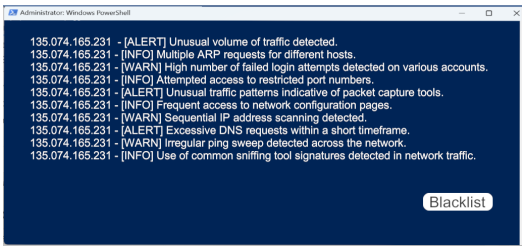


Figure 3.19: Snippet of traffic shown to the participant to teach them how to find an attacker from network traffic.

Locating and Removing Affected Files: Despite blacklisting the attacker, learners discover that the attacker has tampered with the system files. Through interactive challenges, learners narrow down and identify the affected files, ultimately deleting the malicious content to restore system integrity. Snippets of this are seen in Figure 3.20.

The immersive nature of the Sniffing escape room scenario facilitates active learning and knowledge retention among participants. By experiencing the intricacies of cybersecurity defense in a simulated yet realistic environment, learners gain practical skills and insights applicable to real-world scenarios. The Sniffing room exemplifies the seamless integration of scenario-based learning with adaptive VRLE technology. Leveraging user inputs and instructor-defined parameters, the room dynamically adjusts difficulty levels and content presentation to cater to diverse learner backgrounds and proficiency levels. Thus, the Sniffing room scenario within CyEscape exemplifies the efficacy of immersive, scenario-based learning in cybersecurity education. By combining gamified tasks, real-time feedback mechanisms, and adaptive learning principles, our VRLE framework empowers learners to actively engage with and master complex cybersecurity concepts in a dynamic virtual environment.

3.2.4 Performance Evaluation

This section provide a comprehensive analysis of the performance of our RL-based algorithm, followed by insights from the usability study results conducted on a CyEscape implementation.

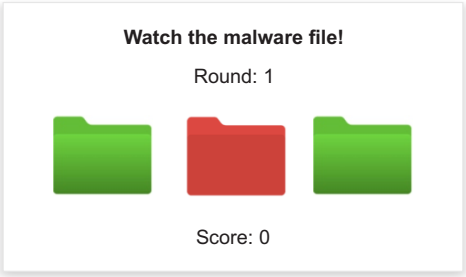


Figure 3.20: Finding the corrupted file post-sniffing attack.

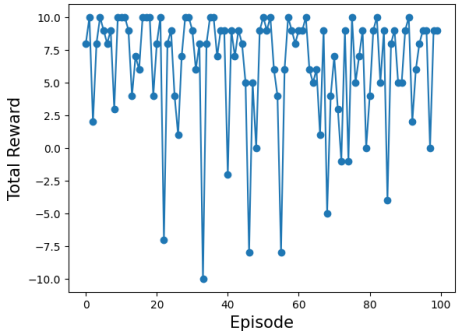


Figure 3.21: Training Progress as seen in the Reward space without DQN policy.

Performance of the RL Algorithm

The performance evaluation of the RL algorithm is crucial to assess its effectiveness in learning and decision-making tasks. The goal of the experiments is to evaluate the extent to which the integration of RL algorithms in CyEscape enhances the learning experience by enabling personalized guidance and adaptive learning experiences for students. Specifically, the aim is to gain insights on how the RL allows the PA to dynamically adapt its strategies based on learner interactions and performance, providing tailored feedback and support. In the context of VR content and guidance for students during cyber attack incident scenarios, the aim is also to study how RL facilitates the development of effective defense mechanisms by optimizing the PA's responses in real-time to ensure that learners receive relevant and timely assistance as they navigate through escape rooms and tackle simulated cyber threats.

Initially, when the RL algorithm operated without employing DQN, the rewards obtained over episodes displayed a fluctuating pattern, suggesting suboptimal learning as shown in Figure 3.21. This observation highlights the necessity of enhancing the learning process. To address this challenge and foster a balance between exploration and exploitation, DQN is integrated into our RL algorithm. DQN is renowned for its effectiveness in heuristic environments characterized by model-free and

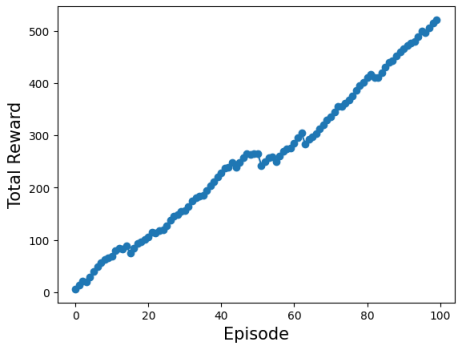


Figure 3.22: Training Progress as seen in the Reward space after employing DQN.

off-policy learning. By leveraging DQN, our PA gained the capability to learn more efficiently from its interactions with the environment. The integration of DQN also facilitated significant improvements in the PA's learning trajectory. Through the iterative refinement of Q-value estimates via experience replay and neural network updates, the PA gradually acquired the ability to make optimal decisions across diverse environments. This combination of exploration and exploitation with DQN contributed to the substantial learning progress and performance enhancement. Figure 3.22 depicts the PA's performance improvement over time, illustrating an upward trend in rewards. This trend signifies the progressive enhancement of the RL-based PA's decision-making abilities and the development of an effective policy.

Usability Study Results

For the usability testing, a cohort of five freshmen students from the Computer Science department was selected as participants. This targeted selection aimed to assess the effectiveness of CyEscape in practical cybersecurity learning within this specific student population. The participants' selection included individuals with varying levels of familiarity with cybersecurity concepts to provide a spectrum of perspectives. Demographic information, such as age and gender, was collected to provide context for the study group.

Usability sessions were conducted in the CyEscape VRLE, utilizing the MetaQuest headset [49] and Unity [50]. Participants engaged with practical cybersecurity concepts, guided by the PA through a simulated sniffing attack scenario. Post-session, participants completed a tailored System Usability Survey (SUS) [59] to assess their VRLE experience. The SUS questionnaire, with 10 questions, provided insights into user engagement, ease of use, consistency, and confidence in navigation. Scores were calculated for a final SUS score ranging from 0 to 100. The survey consisted of the following questions:

1. *I feel motivated to use this VRLE frequently.*
2. *I found the VRLE environment unnecessarily complex.*
3. *The different features and functionalities in this VRLE are well integrated.*
4. *I think I would need the assistance of a technical person to navigate this VRLE effectively.*
5. *I found this VRLE easy to navigate.*
6. *I perceived a high level of consistency in this VRLE.*
7. *I believe most users would quickly learn how to navigate this VRLE.*
8. *I found interacting with this VRLE to be smooth and intuitive.*
9. *I felt confident using this VRLE.*
10. *I had to learn a lot of new things before I could effectively use this VRLE.*

Participant	User 1	User 2	User 3	User 4	User 5
Score	80	82	80	90	79

Table 3.4: SUS scores based on participants feedback.

The SUS scores averaged 82.2 out of 100, indicating generally positive usability perceptions (see Table 4.1). Scores above 68 are deemed above average, while those below suggest below-average usability. Qualitative feedback emphasized the need to simplify complex features and improve user guidance. These findings suggest that CyEscape holds promise as an effective tool for cybersecurity education, particularly among freshmen Computer Science students. Opportunities for refinement exist to further enhance usability and user experience, ensuring the VRLE's effectiveness in supporting cybersecurity learning objectives within this demographic.

3.2.5 Conclusion

This thesis presents the CyEscape framework that provides a promising approach to cybersecurity education, leveraging VR environments and pedagogical agents to enhance learning outcomes for students with diverse backgrounds and knowledge. Through a gamified setting and personalized guidance, CyEscape provides users with immersive experiences that facilitate practical understanding of cyber defense techniques in Escape Rooms designed with realistic cyber attack incident scenarios. Using an RL-based algorithm for the PA demonstrates how adaptive guidance can be tailored

to individual learner needs, promoting engagement and proficiency in cybersecurity concepts. By integrating components such as Google Dialogflow, AWS services, and OpenAI technologies, CyEscape ensures seamless communication and interaction within the VR environment. The usability tests conducted demonstrate CyEscape's effectiveness in delivering engaging and accessible learning experiences. With the potential to scale and adapt to diverse learner profiles, CyEscape holds promise for addressing the growing demand for cybersecurity education in an increasingly digital world.

Future work could involve enhancing CyEscape's adaptability and personalization by refining the RL and conducting longitudinal studies to assess long-term impact. Additionally, the integration of experience-driven and context-driven procedural content generation in the VRLE, building on recent research will enable a more nuanced adaptation to both user interaction and external conditions, offering a highly personalized learning experience where content evolves in real-time to meet each learner's unique needs. Moreover, by incorporating procedural content generation strategies can further make learning more effective and engaging across a wide spectrum of subjects and competencies.

Chapter 4

USABILITY

This section entails the usability results on how RL-agents contribute to both the projects. The agents are used to improve response with feedback affecting the decision making process in the RL algorithm. Within the RISE framework, a web-based service is built to provide seamless interaction with researchers and users working with the SEM instruments. The portal is powered by the RL/IL-agent based chatbot called the RISE-agent that analyzes the CNT image determines the parameter settings i.e., Zoom, Focus and Contrast with the scanned imgage settings i.e., Orientation Loss, Edge Coverage, Distance Entropy, Average Separation and Average Thickness. In the CyEscape framework, a group of students were engaged in the cyber-environment and the participant results were garnered to produce usability.

4.0.1 RISE Usability

To evaluate the effectiveness of our RISE web services approach, a usability study was conducted by following a methodology outlined in [60]. To gather insights on the RISE web services, a user survey was administered comprising three distinct questions, described in the subsequent subsections. A total of 7 researchers participated in this survey, who engaged in activities related to SEM instrumentation operation for CNT synthesis experimentation, and CNT image collection and analysis. The questions below were formulated and answered as described in the examples for each item.

Utility for Automation evaluation

In response to the question *"Did the tool demonstrate how you can achieve insights on image analytics using automation and guided interface compared to manual image analytics process? If so, how?", users had the following comments"* (comments are not syntactically modified in any way):

[1] *"Yes, the tool demonstrated how automation can improve image analytics by using a chatbot to*

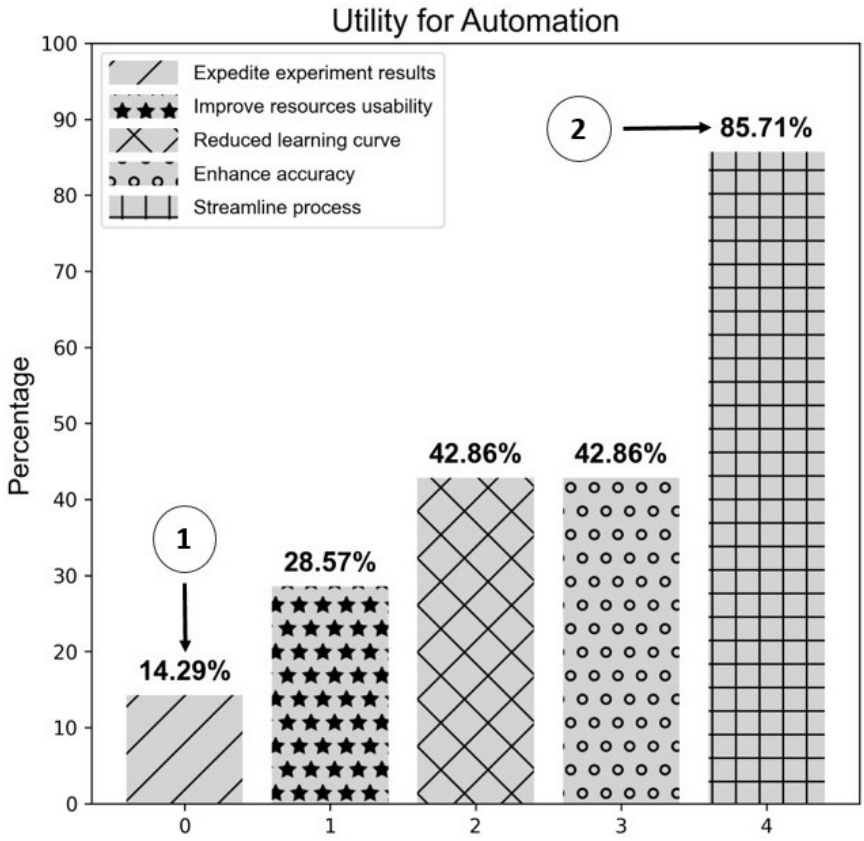


Figure 4.1: Results for the five distinct aspects of research utility for automation showing "Expedite experiment results" being a relatively minor feature (denoted as 1), while "Streamline process" emerges as the major feature (denoted as 2).

recommend parameter adjustments based on image metrics, streamlining the process and enhancing accuracy compared to manual methods."

[2] *"Yes it can. When a local image is uploaded, the chatbot analyzes the image and recommends zoom, focus and contrast iteratively until an image has been produced."*

[4] *"Yes, demonstrates how to access, scan new image and send for analysis on cloud resources automatically."*

Productivity Assistance evaluation

In response to the question *"Did the tool identify any opportunities to improve productivity compared to methods used previously? If so, what were they?", users had the following comments"* (comments are not syntactically modified in any way):

[1] *"The tool offers productivity benefits such as remote instrument control, real-time feedback, and automated tasks, reducing manual intervention, enabling multitasking, and improving efficiency in research processes."*

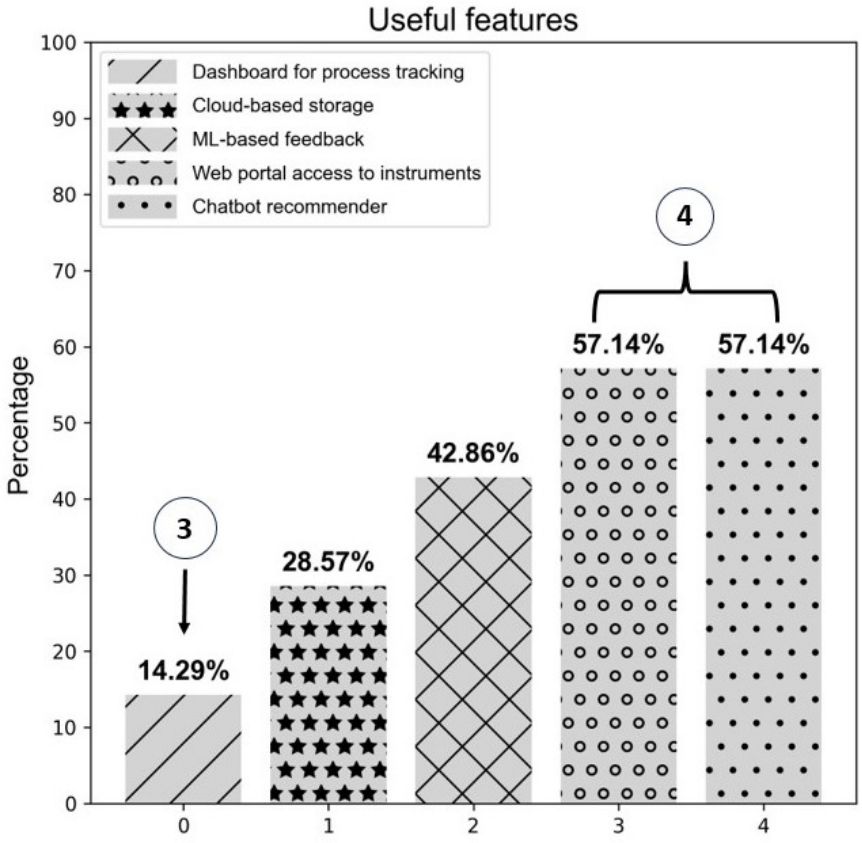


Figure 4.2: Results for the useful features for user experience across five distinct aspects showing "Dashboard for process tracking" is considered a minor feature (denoted as 3), while both "Chatbot recommender" and "web service access to instruments" emerge as major features (denoted as 4).

[2] *"The tool offers productivity benefits such as remote instrument control, real-time feedback, and automated tasks, reducing manual intervention, enabling multitasking, and improving efficiency in research processes."*

[4] *"Yes, earlier methods would involve several manual steps for data storage, transfer and launching analysis. The tool cuts down many of these steps and so can increase productivity significantly."*

Useful Features evaluation

In response to the question *"Were there any features within the tool that stood out as particularly useful? ", users had the following comments* (comments are not syntactically modified in any way):

[1] *"Key features include the chatbot for real-time recommendations, remote instrument control via a web service, machine learning for optimization, cloud-based storage, and a dashboard for tracking progress, enhancing the overall research experience."*

[2] *"Remote Access and Real-time feedback particularly stood out. Automating the whole pipeline increases efficiency".*

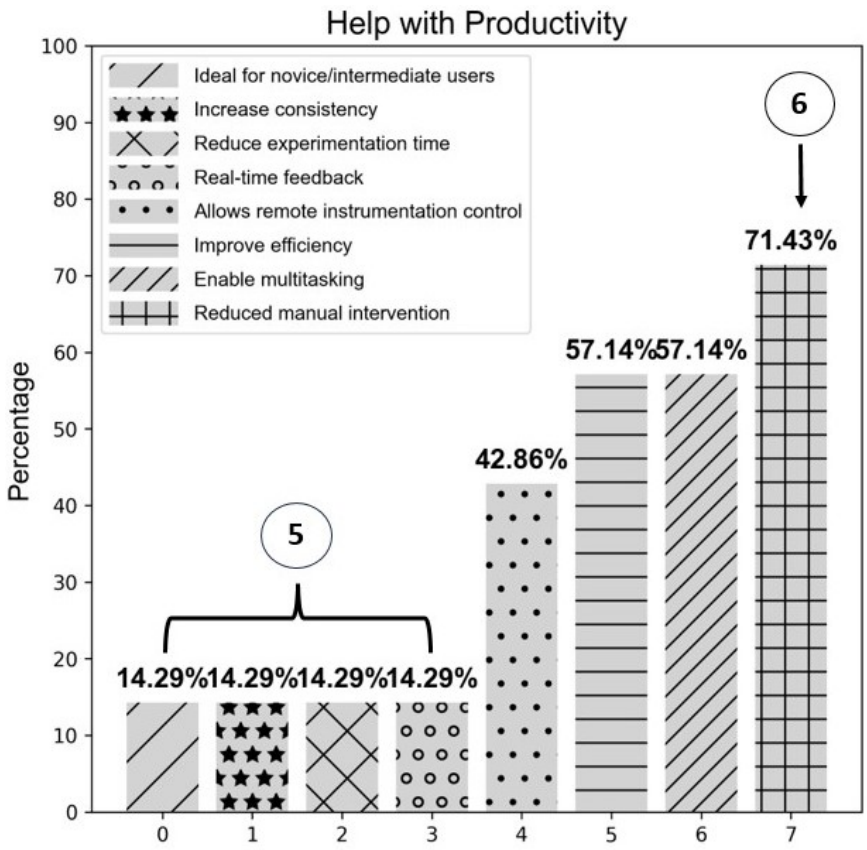


Figure 4.3: Results for the impact on productivity across eight distinct aspects showing four features, namely "ideal for novice intermediate users," "Increase consistency," "Reduce experimentation time," and "Real-time feedback," are considered relatively minor (denoted as 5); Conversely, the feature "Reduced manual intervention" is deemed a major asset (denoted as 6).

[4] *"Recommendations provided and interactions with chatbot to do so are good functionalities."*

4.0.2 Results discussion

Figures 4.1, 4.2 and 4.3 present the synthesized survey responses to each question in three separate bar plots. These plots depict the primary and minor elements of the online site based on survey responses. In Figure 4.1, responses to the question Utility for Automation evaluation are presented in five distinct aspects of "Enhance accuracy", "Expedite experiment results", "Improve resource usability", "Reduced learning curve", "Streamline process" where "Expedite experiment results" is considered as a minor feature, around 14.29% support (denoted as 1), while "Streamline process" as the predominant feature, commanding approximately 85.71% support (denoted as 2).

In Figure 4.2, responses to the question Useful Features evaluation are represented in five distinct aspects known as "Chatbot recommender", "web service access to instruments", "Dashboard for process tracking", "ML-based feedback", and "Cloud-based storage". "Dashboard for process

tracking" is considered a minor feature, securing 14.19% support (denoted as 3), while both "Chatbot recommender" and "web service access to instruments" emerge as major features, each receiving approximately 57.14% support (denoted as 4).

Figure 4.3 assesses the RISE web services impact on productivity across eight distinct aspects "Allows remote instrumentation control", "Real-time feedback", "Reduced manual intervention", "Enable multitasking", "Improves efficiency", "Increase consistency", "Ideal for novice/intermediate users", and "Reduce experimentation time". Four features, namely "ideal for novice intermediate users," "Increase consistency," "Reduce experimentation time," and "Real-time feedback," are considered relatively minor, each obtaining 14.29% support (denoted as 5). Conversely, the feature "Reduced manual intervention" is deemed a major asset, commanding an impressive 71.43% support (denoted as 6).

4.0.3 CyEscape Usability

For the usability testing, a cohort of five freshmen students from the Computer Science department was selected as participants. This targeted selection aimed to assess the effectiveness of CyEscape in practical cybersecurity learning within this specific student population. The participants' selection included individuals with varying levels of familiarity with cybersecurity concepts to provide a spectrum of perspectives. Demographic information, such as age and gender, was collected to provide context for the study group.

Usability sessions were conducted in the CyEscape VRLE, utilizing the MetaQuest headset [49] and Unity [50]. Participants engaged with practical cybersecurity concepts, guided by the PA through a simulated sniffing attack scenario. Post-session, participants completed a tailored System Usability Survey (SUS) [59] to assess their VRLE experience. The SUS questionnaire, with 10 questions, provided insights into user engagement, ease of use, consistency, and confidence in navigation. Scores were calculated for a final SUS score ranging from 0 to 100. The survey consisted of the following questions:

1. *I feel motivated to use this VRLE frequently.*
2. *I found the VRLE environment unnecessarily complex.*
3. *The different features and functionalities in this VRLE are well integrated.*
4. *I think I would need the assistance of a technical person to navigate this VRLE effectively.*
5. *I found this VRLE easy to navigate.*

6. *I perceived a high level of consistency in this VRLE.*

7. *I believe most users would quickly learn how to navigate this VRLE.*

8. *I found interacting with this VRLE to be smooth and intuitive.*

9. *I felt confident using this VRLE.*

10. *I had to learn a lot of new things before I could effectively use this VRLE.*

Participant	User 1	User 2	User 3	User 4	User 5
Score	80	82	80	90	79

Table 4.1: SUS scores based on participants feedback.

The SUS scores averaged 82.2 out of 100, indicating generally positive usability perceptions (see Table 4.1). Scores above 68 are deemed above average, while those below suggest below-average usability. Qualitative feedback emphasized the need to simplify complex features and improve user guidance. These findings suggest that CyEscape holds promise as an effective tool for cybersecurity education, particularly among freshmen Computer Science students. Opportunities for refinement exist to further enhance usability and user experience, ensuring the VRLE's effectiveness in supporting cybersecurity learning objectives within this demographic.

Chapter 5

CONCLUSION

This thesis leverages intelligent RL and MARL agents in heuristic settings for both RISE and CyEscape. The learning curves for both the projects suggest RL's potential to capitulate rewards in these dynamic environments and showcase RL's potential to learn and thrive in a Markov's process.

The RISE framework successfully addresses performance improvement and data/instruments security during image analytics tasks, providing seamless and secure communication for remote access to scientific instruments. The implemented RL agent-based approach to identify the optimal learning method for guiding real-time image processing tasks during in-situ CNT manufacturing on cyber-enabled SEM instruments shows learning curve to learn from the environment and make decisions in real-time.

RL enabled Pedagogical Agents in Cyescape demonstrates how adaptive guidance can be tailored to individual learner needs, promoting engagement and proficiency in cybersecurity concepts. By integrating components such as Google Dialogflow, AWS services, and OpenAI technologies, CyEscape ensures seamless communication and interaction within the VR environment. The usability tests conducted demonstrate CyEscape's effectiveness in delivering engaging and accessible learning experiences. With the potential to scale and adapt to diverse learner profiles, CyEscape holds promise for addressing the growing demand for cybersecurity education in an increasingly digital world. The RL agents also show case how dynamic adaptibility in VR can be levaraged to adapt to individual students by adapting to their performance.

The successful implementation of RL in these frameworks highlights its potential to significantly enhance scientific workflows and educational experiences. By automating complex processes and providing adaptive, real-time optimization, RL not only improves efficiency and outcomes but also paves the way for further technological advancements.

Chapter 6

FUTURE WORKS

Future work aims to build on the successes of the RISE and CyEscape frameworks, leveraging the potential of RL to further enhance scientific workflows and educational experiences. By advancing RL algorithms, expanding application scopes, and improving user experiences, we can unlock new possibilities and drive innovation across diverse fields.

In material discovery, RL can be leveraged to provide iterative feedback control to predict and recommend parameters for improving the quality of CNT images based on the characterization of ideal CNT image parameters. Additionally, expanding the RISE system with web services that integrate our RL/IL agents for a broader range of image analytics applications and CNT synthesis control is a promising direction. This expansion could involve controlling the CNT growth rate based on current growth rate and SEM chamber conditions, such as temperature and pressure.

Similarly, in the CyEscape framework and in VR, studies can be conducted on adaptability and personalization by refining the RL and conducting longitudinal studies to assess long-term impact.Additionally, the integration of experience-driven and context-driven procedural content generation in the VRLE, building on recent research will enable a more nuanced adaptation to both user interaction and external conditions, offering a highly personalized learning experience where content evolves in real-time to meet each learner's unique needs.

RL agents can further enhance scientific workflows and educational experiences with their adaptability to diverse environment. By advancing RL algorithms, expanding application scopes, and improving user experiences, we can unlock new possibilities and drive innovation across diverse fields.

BIBLIOGRAPHY

[1] P. Nguyen, T. Elgamal, S. Konstanty, T. Nicholson, S. Turner, P. Su, K. Nahrstedt, T. Spila, R. H. Campbell, J. Dallesasse *et al.*, "Bracelet: Edge-cloud microservice infrastructure for aging scientific instruments," in *2019 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2019, pp. 692–696.

[2] P. Calyam, A. Kalash, R. Gopalan, S. Gopalan, and A. Krishnamurthy, "Rice: A reliable and efficient remote instrumentation collaboration environment," *Advances in Multimedia*, vol. 2008, 2008.

[3] T. Hajilounezhad, R. Bao, K. Palaniappan, F. Bunyak, P. Calyam, and M. R. Maschmann, "Predicting carbon nanotube forest attributes and mechanical properties using simulated images and deep learning," *npj Computational Materials*, vol. 7, no. 1, p. 134, 2021.

[4] K. Ahn, Z. Mhammedi, H. Mania, Z.-W. Hong, and A. Jadbabaie, "Model predictive control via on-policy imitation learning," in *Learning for Dynamics and Control Conference*. PMLR, 2023, pp. 1493–1505.

[5] W. Lei, H. Wen, J. Wu, and W. Hou, "Maddpg-based security situational awareness for smart grid with intelligent edge," *Applied Sciences*, vol. 11, no. 7, p. 3101, 2021.

[6] Z. Cheng, M. Min, M. Liwang, L. Huang, and Z. Gao, "Multiagent ddpg-based joint task partitioning and power control in fog computing networks," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 104–116, 2022.

[7] P. Nguyen, S. Konstanty, T. Nicholson, T. O'brien, A. Schwartz-Duval, T. Spila, K. Nahrstedt, R. H. Campbell, I. Gupta, M. Chan *et al.*, "4ceed: Real-time data acquisition and analysis framework for material-related cyber-physical environments," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*. IEEE, 2017, pp. 11–20.

[8] J. Bouvette, Q. Huang, A. Bartesaghi, and M. J. Borgnia, "Smartscope: Ai-driven grid navigation for high-throughput cryo-em," in *2021 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, 2021, pp. 1–6.

[9] B. Huang, Z. Li, and J. Li, "An artificial intelligence atomic force microscope enabled by machine learning," *Nanoscale*, vol. 10, no. 45, pp. 21 320–21 326, 2018.

[10] A. Neumann, S. Welten, J. Kunz, R. Klamma, and S. Decker, "Haico: A monitoring and transaction chatbot for distributed analytics workflows," in *2023 IEEE International Conference on Web Services (ICWS)*, 2023, pp. 707–709.

[11] J. L. Plass, B. D. Homer, and C. K. Kinzer, "Foundations of game-based learning," *Educational psychologist*, vol. 50, no. 4, pp. 258–283, 2015.

[12] N. El Mawas, M. Bratu, D. Caraman, and C. H. Muntean, "Investigating the learning impact of game-based learning when teaching science to children with special learning needs," in *Society for Information Technology & Teacher Education International Conference*. Association for the Advancement of Computing in Education (AACE), 2019, pp. 2371–2377.

[13] N. Shaker, J. Togelius, and M. J. Nelson, "Procedural content generation in games," 2016.

[14] V. Bogicevic, S. Seo, J. A. Kandampully, S. Q. Liu, and N. A. Rudd, "Virtual reality presence as a preamble of tourism experience: The role of mental imagery," *Tourism Management*, vol. 74, pp. 55–64, 2019.

[15] E. Löffler, B. Schneider, T. Zanwar, and P. M. Asprion, "Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness," *International Journal of Serious Games*, vol. 8, no. 1, pp. 59–70, 2021.

[16] J. E. DeBello, S. Schmeelk, D. M. Dragos, E. Troja, and L. M. Truong, "Teaching effective cybersecurity through escape the classroom paradigm," in *2022 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2022, pp. 17–23.

[17] A. M. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches," *Symmetry*, vol. 15, no. 12, p. 2175, 2023.

[18] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*. IEEE, 2012, pp. 256–262.

[19] M. Schmidt, N. Glaser, C. Schmidt, R. Kaplan, H. Palmer, and S. Cobb, "Programming for generalization: Confronting known challenges in the design of virtual reality interventions for autistic users," *Computers & Education: X Reality*, vol. 2, p. 100013, 2023.

[20] X. Wang and W. Xing, "Supporting youth with autism learning social competence: A comparison of game-and nongame-based activities in 3d virtual world," *Journal of educational computing research*, vol. 60, no. 1, pp. 74–103, 2022.

[21] S. V. Veneruso, L. S. Ferro, A. Marrella, M. Mecella, and T. Catarci, "Cybervr: an interactive learning experience in virtual reality for cybersecurity related issues," in *Proceedings of the International Conference on Advanced Visual Interfaces*, 2020, pp. 1–8.

[22] S. S. Nuguri, P. Calyam, R. Oruche, A. Gulhane, S. Valluripally, J. Stichter, and Z. He, "vsocial: a cloud-based system for social virtual reality learning environment applications in special education," *Multimedia Tools and Applications*, vol. 80, pp. 16 827–16 856, 2021.

[23] G. Veletsianos, C. Miller, and A. Doering, "Enali: A research and design framework for virtual characters and pedagogical agents," *Journal of Educational Computing Research*, vol. 41, no. 2, pp. 171–194, 2009.

[24] N. Glaser, "Exploring the potential of chatgpt as an educational technology: An emerging technology report," *Technology, Knowledge and Learning*, vol. 28, no. 4, pp. 1945–1952, 2023.

[25] N. K. H. Chia and J. Li, "Design of a generic questionnaire for reflective evaluation of a virtual reality-based intervention using virtual dolphins for children with autism." *International Journal of Special Education*, vol. 27, no. 3, pp. 45–53, 2012.

[26] S. L. Burke, T. Bresnahan, T. Li, K. Epnere, A. Rizzo, M. Partin, R. M. Ahlness, and M. Trimmer, "Using virtual interactive training agents (vita) with adults with autism and other developmental disabilities," *Journal of autism and developmental disorders*, vol. 48, pp. 905–912, 2018.

[27] W. L. Johnson, J. Rickel, R. Stiles, and A. Munro, "Integrating pedagogical agents into virtual environments," *Presence*, vol. 7, no. 6, pp. 523–546, 1998.

[28] A. S. D. Martha and H. B. Santoso, "The design and impact of the pedagogical agent: A systematic literature review." *Journal of educators Online*, vol. 16, no. 1, p. n1, 2019.

[29] T. Hajilounezhad, D. M. Ajiboye, and M. R. Maschmann, "Evaluating the forces generated during carbon nanotube forest growth and self-assembly," *Materialia*, vol. 7, p. 100371, 2019.

[30] N. P. Nguyen, I. Ersoy, J. Gotberg, F. Bunyak, and T. A. White, "Drpnet: automated particle picking in cryo-electron micrographs using deep regression," *BMC bioinformatics*, vol. 22, no. 1, pp. 1–28, 2021.

[31] D. Wei, Z. Lin, D. Franco-Barranco, N. Wendt, X. Liu, W. Yin, X. Huang, A. Gupta, W.-D. Jang, X. Wang *et al.*, "Mitoem dataset: large-scale 3d mitochondria instance segmentation from em images," in *International Conference on Medical Image Computing and Computer-Assisted Intervention*. Springer, 2020, pp. 66–76.

[32] R. Hines, T. Hajilounezhad, C. Love-Baker, G. Koerner, and M. R. Maschmann, "Growth and mechanics of heterogeneous, 3d carbon nanotube forest microstructures formed by sequential selective-area synthesis," *ACS applied materials & interfaces*, vol. 12, no. 15, pp. 17 893–17 900, 2020.

[33] J. Mireles, C. Terrazas, S. M. Gaytan, D. A. Roberson, and R. B. Wicker, "Closed-loop automatic feedback control in electron beam melting," *The International Journal of Advanced Manufacturing Technology*, vol. 78, pp. 1193–1199, 2015.

[34] T. Osa, C. Staub, and A. Knoll, "Framework of automatic robot surgery system using visual servoing," in *2010 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2010, pp. 1837–1842.

[35] N. P. Nguyen, R. Surya, M. Maschmann, P. Calyam, K. Palaniappan, and F. Bunyak, "Self-supervised orientation-guided deep network for segmentation of carbon nanotubes in sem imagery," in *Computer Vision–ECCV 2022 Workshops: Tel Aviv, Israel, October 23–27, 2022, Proceedings, Part VIII*. Springer, 2023, pp. 412–428.

[36] "Scanning electron microscopy," https://www.nanoscience.com/techniques/scanning-electron-microscopy/, accessed: Jan 12, 2024.

[37] R. Lowe, Y. Wu, A. Tamar, J. Harb, P. Abbeel, and I. Mordatch, "Multi-agent actor-critic for mixed cooperative-competitive environments," 2020.

[38] A. Kambhampati. (2023) Marl: Rl code to provide parameter feedback. Dataset, 2023. Accessed: October 26, 2023. Available at http://bit.ly/3SHx0yU. [Online]. Available: https://shorturl.at/xN467

[39] A. Pandey, R. Surya, M. Maschmann, and P. Calyam, "Reinforcement learning based carbon nanotube growth automation," in *2021 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*. IEEE, 2021, pp. 1–10.

[40] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A Review on Authentication Methods," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 5, pp. 95–107, Mar. 2013. [Online]. Available: https://hal.science/hal-00912435

[41] M. R. Mesbahi, A. M. Rahmani, and M. Hosseinzadeh, "Reliability and high availability in cloud computing environments: a reference roadmap," *Human-centric Computing and Information Sciences*, vol. 8, pp. 1–31, 2018.

[42] Imitation Learning Code and Dataset, 2023. Accessed: October 26, 2023. Available at https://bit.ly/ImitationLearningCodeAndDataset. [Online]. Available: https://github.com/melemus/rise_environment/blob/216ee41e224239ee3bb2845726c21c9fb10797b5/ImitationLearning_Repo/IL_Code_NewDataset.ipynb

[43] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The emerging threat of ai-driven cyber attacks: A review," *Applied Artificial Intelligence*, vol. 36, no. 1, p. 2037254, 2022.

[44] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, vol. 72, pp. 212–233, 2018.

[45] A. Alexiou and M. C. Schippers, "Digital game elements, user experience and learning: A conceptual framework," *Education and Information Technologies*, vol. 23, pp. 2545–2567, 2018.

[46] Y. Li, "Deep reinforcement learning: An overview," *arXiv preprint arXiv:1701.07274*, 2017.

[47] K. B. Vekaria, P. Calyam, S. Wang, R. Payyavula, M. Rockey, and N. Ahmed, "Cyber range for research-inspired learning of "attack defense by pretense" principle and practice," *IEEE Transactions on Learning Technologies*, vol. 14, no. 3, pp. 322–337, 2021.

[48] T. Brown, B. Mann, N. Ryder, M. Subbiah, J. D. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell *et al.*, "Language models are few-shot learners," *Advances in neural information processing systems*, vol. 33, pp. 1877–1901, 2020.

[49] I. Meta Platforms, "Meta quest 2," https://www.meta.com/quest-2/, 2020, accessed: 2024-07-02.

[50] U. S. Assets", "Unity asset store, 2022," https://assetstore.unity.com/, 2022.

[51] J. C. Snyder, *A framework and exploration of a cybersecurity education escape room.* Brigham Young University, 2018.

[52] C. Decusatis, B. Gormanly, E. Alvarico, O. Dirahoui, J. McDonough, B. Sprague, M. Maloney, D. Avitable, and B. Mah, "A cybersecurity awareness escape room using gamification design principles," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC).* IEEE, 2022, pp. 0765–0770.

[53] Z. Merchant, E. T. Goetz, L. Cifuentes, W. Keeney-Kennicutt, and T. J. Davis, "Effectiveness of virtual reality-based instruction on students' learning outcomes in k-12 and higher education: A meta-analysis," *Computers & education*, vol. 70, pp. 29–40, 2014.

[54] L. Dai, M. M. Jung, M. Postma, and M. M. Louwerse, "A systematic review of pedagogical agent research: Similarities, differences and unexplored aspects," *Computers & Education*, vol. 190, p. 104607, 2022.

[55] U. A. Store", "Meta xr all-in-one sdk for unity execution in metaquest headsets [asset package]," https://assetstore.unity.com/packages/tools/integration/meta-xr-all-in-one-sdk-269657, 2022, accessed: 2024-07-02.

[56] "OpenAI", "Openai plugin for unity, 2022," https://github.com/srcnalt/OpenAI-Unity, 2022, accessed: 2024-07-02.

[57] Google, "Google, "dialogflow," [online]," https://dialogflow.cloud.google.com/, 2020, accessed: 2024-07-02.

[58] A. W. Services, "Amazon web services, "amazon polly,"," https://aws.amazon.com/polly/, 2020, accessed: 2024-07-02.

[59] J. Brooke *et al.*, "Sus-a quick and dirty usability scale," *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996.

[60] M. Kejriwal and P. Szekely, "mydig: Personalized illicit domain-specific knowledge discovery with no programming," *Future Internet*, vol. 11, no. 3, p. 59, 2019.