PROXIMA : Process Rather than Outcome, eXplainable Instruction of Multiple Ai for Cybersecurity Exercise

Sung-Kyu Ahn[1] and Ki-Woong Park[2*]

[1] SysCore Lab, Sejong University,Seoul, Korea
yiimfn@gmail.com
[2] Department of Computer and Information Security, Sejong University, Seoul, Korea
woongbak@sejong.ac.kr

Abstract

The increasing complexity and scale of cyber threats, driven by advances in AI, IoT, and cloud computing, have created a need for highly skilled cybersecurity professionals. Current cybersecurity training solutions face limitations in addressing the dynamic nature of threats, lacking real-time adaptability and personalized learning experiences. This paper introduces CENTAURI, a conceptual platform that leverages multiple LLMs to create dynamic, cloud-based cybersecurity training environments. CENTAURI aims to provide personalized learning experiences by adapting difficulty levels and content in real-time, utilizing LLM-driven behavioral analysis. The proposed architecture integrates infrastructure management, trainee analysis, and feedback generation modules, each operating as a Multi-Agent System following the MAPE-K process. By automating the generation and management of training infrastructure, CENTAURI conceptually addresses the resource-intensive nature of cybersecurity training while enhancing the potential effectiveness of the learning process. This paper presents the theoretical framework of CENTAURI, discussing its potential benefits and challenges in revolutionizing cybersecurity education.

Keywords: Cyber Range, Cybersecurity Exercise, LLM, Generative AI

1 Introduction

With the rapid increase in the complexity, frequency, and scale of damage from cyber threats based on various IT technologies such as AI, IoT, and cloud computing, there is a growing need for security professionals to carry out cybersecurity missions. Professionals working in the field of cybersecurity need to be capable of making appropriate decisions by utilizing diverse fields of knowledge and data learned through extensive experience to respond to cyber threats[6]. However, gaining experience in reviewing and responding to various cyber threats in real-world environments remains a challenging task[5].

Against this backdrop, creating a cyber security training environment to enhance effective response capabilities in real-world scenarios through practical experience and systematic security technology learning has emerged as an urgent issue. Yet, existing cybersecurity training generation technologies face limitations in fully addressing the rapidly changing cybersecurity landscape. In particular, improvements are needed in providing personalized learning experiences, enhancing real-time response capabilities, and managing resources efficiently[15, 13, 16, 4].

Current cybersecurity training environments can be broadly classified into 'simulation-based platforms' and 'education-based platforms', each with its own strengths and limitations. Simulation-based platforms, such as CDX(Cyber Defense Exercise), Cyber Range, and CTF(Capture The Flag), provide realistic training experiences through virtual environments

---

*corresponding author

that closely resemble actual conditions. While these platforms offer valuable real-world scenario experience, they are resource-intensive, have limited scalability, and often employ inflexible evaluation methods. On the other hand, education-based platforms, including training platforms and e-learning systems, offer systematic and step-by-step learning through lectures, exercises, and online modules. These platforms provide efficient, personalized learning but lack real-time response training, often have a gap between training and real-world environments, and struggle with limited interactivity. Despite their respective advantages, both approaches still face challenges in fully addressing the rapidly evolving cybersecurity threat landscape.

In this paper, we propose CENTAURI (Cybersecurity Exercise aNd Training Archtecture Using Redesign and Interaction), a cybersecurity training platform that integrates multiple LLMs to overcome the limitations of existing training environments and provide an efficient training environment. CENTAURI offers cybersecurity training based on cloud environments and provides dynamic, personalized training experiences by utilizing multiple LLMs, based on analysis function, leveraging pattern recognition and inference capabilities from LLM, to provide real-time behavior analysis, personalized difficulty adjustment, tailored learning feedback, and comprehensive evaluation reports. CENTAURI is expected to enhance efficiency in the cybersecurity training process by automating the training and feedback generation for cybersecurity professionals, while also contributing to cost reduction in building training environments.

The structure of this paper is as follows. in Section 2, we provide a detailed analysis of related research and the limitations of existing cybersecurity training platform technologies. Section 3, explains the structure and operational principles of CENTAURI, along with a discussion of the technical details required for its implementation. Finally, in Section 4, we conclude by outlining the limitations of CENTAURI, proposing future research directions, and discussing the potential and trajectory of next-generation cybersecurity training platforms.

2 Background and related work

Research on the efficient construction and implementation of cybersecurity training environments has been continuously conducted. In this section, we analyze and compare prior studies related to the core propositions of CENTAURI.

2.1 Cybersecurity Exercise and Training

Cybersecurity training programs provide trainees with technical education on cybersecurity skills and offer practical and simulation environments where these skills can be applied. Currently, many organizations and companies operate various cybersecurity training programs and systems to cultivate cybersecurity professionals. These cybersecurity training environments can be broadly classified into 'simulation-based platforms' and 'Education-based platforms'.

'Simulation-based platform's provide realistic training experiences through virtual environments that closely resemble actual conditions. Notable examples include the 'CDX', 'Cyber Range', and 'CTF'. The Cyber Range is a platform where trainees can experience cyber attack and defense scenarios in a virtual network environment that simulates real-world conditions. While this approach offers trainees a realistic training experience and helps them develop appropriate response capabilities in real-world situations, it requires significant time, cost, and human resources to configure various scenarios and infrastructure [5]. Moreover, simulation-based platforms generally use outcome-based scoring systems, making it difficult to consider the specific evaluation and skill levels of participants [15, 10].

'Education-based platforms' provide trainees with systematic and step-by-step learning and practice through lectures, exercises, and e-learning. Notable examples include 'Training Platforms' and 'e-learning.' These platforms offer the advantage of allowing participants to engage in efficient, personalized learning tailored to their individual capabilities. However, unlike simulation-based platforms, they face limitations in training real-time response capabilities due to the static nature of scenarios and the gap between training and real-world environments[16, 4].

2.2   Automated Evaluation for Cybersecurity Trainees

Research on automate performance evaluation and analysis methods has been continuously conducted in conjunction with the development of cybersecurity training environment configuration.

Švábenský [14] conducted research on methods for collecting training data, analyzing it, evaluating it, and generating feedback in cybersecurity training environments. This research focused on the process of collecting learner activity data, analyzing it, and generating appropriate feedback. Using the KYPO CRP training portal, user training data is collected, and the analysis process identifies errors and anomalous behaviors. Through this process, appropriate stepwise feedback is generated for training participants, enhancing their understanding of the training content and suggesting directions for improvement.

Glas et al. [6] addressed the evaluation challenges of the cybersecurity training environment, CRX(Cyber Range Exercise). In their study, they proposed the TARGET framework to systematically evaluate the effectiveness of CRX. The study offers a structured evaluation methodology and a comparison framework for CRX. The TARGET framework consists of a taxonomy for classifying evaluation criteria and an evaluation process, supporting CRX designers in making continuous improvements. The study demonstrated significant improvements in the learning outcomes and experiences of 50 participants who engaged in the Iceberg CRX.

Abbott et al. [1] conducted research applying automated performance evaluation techniques to cybersecurity training exercises. Their study collected and analyzed participants' activity data during the Tracer FIRE (Forensic Incidence Response Exercise), assessing individual performance and proposing a framework to automate evaluation by modeling participant activity data. This research enabled automatic log data analysis, allowing for real-time identification of issues and feedback generation for training participants.

These related studies highlight the lack of efficient evaluation methods and standardized feedback in existing cybersecurity training environments. They propose effective feedback generation based on the analysis of participants' activity data. However, to generate feedback data, these approaches rely on task completion and interaction data from the cybersecurity training environment. While this allows for optimized stepwise evaluation and feedback generation for specific scenarios, it presents limitations in providing personalized analysis and feedback tailored to individual participants.

2.3   Automated Infrastructure Generation

In order to dynamically control the training infrastructure in cybersecurity training environments, a combination of control interfaces for the infrastructure and real-time infrastructure information analysis technologies must be considered. Previous studies have focused on controlling and generating infrastructure for cloud systems and separate virtualization systems.

Huff et al. [7] proposed CyberArena, which is designed to allow users to define and deploy lab environments in a user-friendly manner using YAML file formats. CyberArena controls

cloud resources using the cloud provider's API, dynamically creating, managing, and deleting resources according to the user's needs. This enables instructors to detect and assess whether specific tasks have been completed.

Kwon et al. [8] evaluated the performance of LLMs(Large Language Models) such as Chat-GPT and Bard on 58 Ansible script modification cases of OSS(open-source software). Their study found that LLMs provided helpful responses in 70% of the sampled cases.

Leitner et al. [9] emphasized the need for a flexible and scalable AIT Cyber Range to support cybersecurity training, exercises, and research. The AIT Cyber Range utilizes open-source technologies and is composed of four key components: computing platform, infrastructure provisioning, software delivery, and scenario engine. The scenario engine, GameMaker, which is custom-developed, controls the flow of cyber exercise scenarios.

2.4   Application of Generative AI and LLMs

Generative AI and LLM refers to LLMs capable of generating new data. These models are trained on datasets ranging from tens to hundreds of terabytes and are capable of performing a wide variety of tasks based on extensive knowledge. Previous studies have focused on efficiently utilizing LLM and ensuring the accuracy of its output data.

Nascimento et al. [12] introduced the 'GPT-in-the-loop' approach, which investigates the reasoning capabilities of LLMs like GPT(Generative Pre-trained Transformers) within MAS(Multi-agent Systems). This framework aims to enhance problem-solving and explanation abilities using GPT-4. The approach was applied to a smart streetlight application, leveraging autonomous agents to create an energy-efficient lighting system. With GPT-4 integration, these agents demonstrated improved decision-making and adaptability.

Akuthota et al. [2] conducted an experiment using the GPT-3.5-Turbo model to detect security vulnerabilities in code snippets. In 2,740 test cases, the model achieved an accuracy of 0.77, suggesting its potential as a useful tool for vulnerability prediction. However, the experiment also emphasized the need for continuous improvement in the model's methodology.

Naito et al. [11] aimed to demonstrate the effectiveness of a system that inputs asset management data and vulnerability information into ChatGPT to identify high-threat attack paths. The experiment results confirmed that the system could effectively discover cybersecurity threats within organizations and provide useful attack paths for risk assessment.

3   Design

This study hypothesizes that the CENTAURI-based training environment can provide a dynamic and personalized cybersecurity training system based on diverse learning data, while serving as an AI-driven tutor throughout the training process. In this section, we outline the specific implementation methods of CENTAURI designed to validate this hypothesis.

3.1   Main Structure of CENTAURI

As shown in Figure 1, CENTAURI is composed of Infrastructure, Adapter, and Core, based on the CENTAURI Server. The CENTAURI Infrastructure is built on an OpenStack cluster environment, virtualizing the cloud-based cybersecurity training environment. Each computing environment within the CENTAURI Infrastructure consists of a pseudo terminal, which collects and stores real-time process and network information based on trainee input, and a
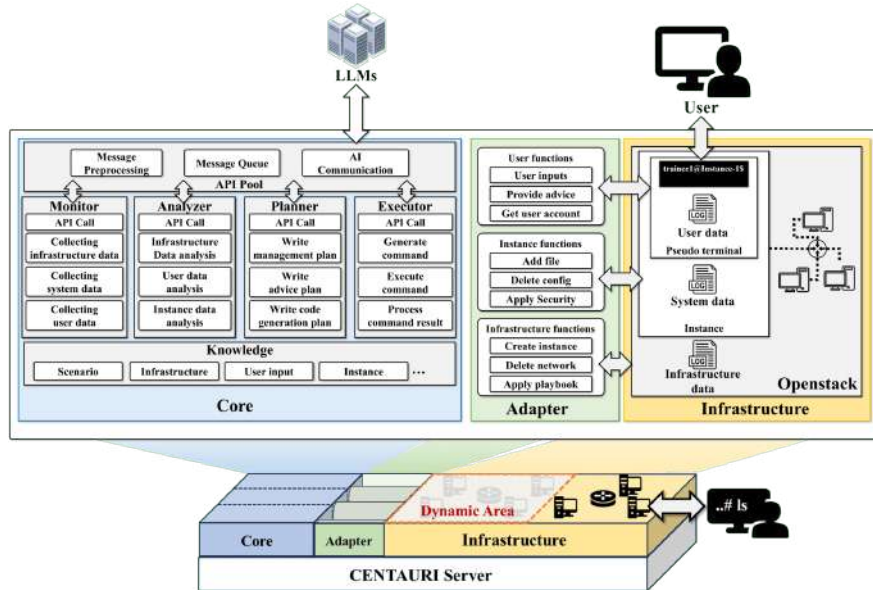
Figure 1: Structure of the CENTAURI Platform

Guest OS for cybersecurity training. CENTAURI Adapter store system and trainee information collected from the pseudo terminal within the infrastructure, as well as infrastructure data collected in real-time from the OpenStack environment. They function as a set of methods for transmitting and receiving data, collecting and delivering information requested by the Core. CENTAURI Core is composed of multiple parallel modules, each serving a specific purpose: real-time infrastructure control, real-time trainee analysis, and real-time feedback generation. Each module within the Core is structured as a MAS, composed of multiple agents that perform the MAPE-K(Monitor, Analyze, Plan, Execute, and Knowledge) processes.
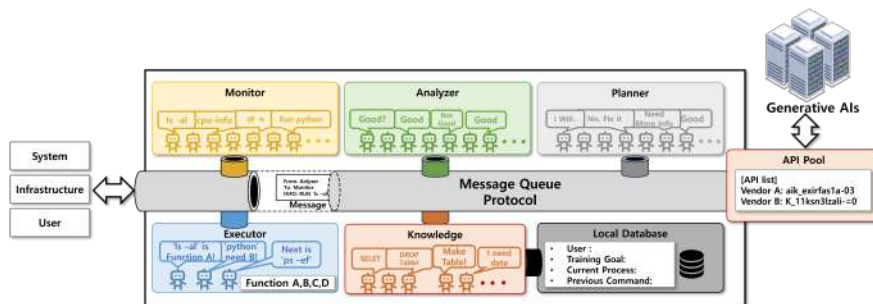

Figure 2: Detailed Structure of CENTAURI Core

As shown in Figure 2, CENTAURI-Core directly communicates with LLM and is composed of multiple-agents that perform the collection, analysis, planning, and execution using the MAPE-K Loop model for efficient data management, analysis, and inference based on information collected from the infrastructure and trainee data. This architecture makes the CENTAURI-Core module the central component for executing core operations, where data is

generated according to the needs of each agent. The agents interact with each other via a message queue, focusing on their respective roles, and ultimately generate data that controls the CENTAURI-Infrastructure through the CENTAURI-Adapter. The structure and description of each agent are as follows:

3.1.1   Detailed Structure of CENTAURI Core

- `API Pool`– The API Pool serves as the hub for communicating with multiple LLM services. API Pool transmits requests to different AI models simultaneously, aggregates their responses, and distributes the processed results to relevant components according to the message protocol.

- `Monitor`– The Monitor employs multiple LLMs to continuously collect and interpret data from the infrastructure, instance systems, and trainee interactions within the CENTAURI environment. These AI models work in parallel to perform real-time gathering and initial analysis of various metrics, including system performance indicators, network traffic, resource utilization statistics, and trainee input data.

- `Analyzer`– The Analyzer leverages an ensemble of LLMs, each employing different pattern recognition and inference techniques. These models work concurrently to verify and select the most optimal data based on monitored inputs. They collaboratively verify monitoring items, plans, and execution results, analyzing trainee input and infrastructure data to ensure accuracy and relevance.

- `Planner`– The Planner utilizes a diverse set of LLMs to design the next set of actions within CENTAURI. Each AI model generates initial plans independently, focusing on different aspects or using various strategies. These plans are then evaluated and combined by the Analyzer's AI ensemble to produce a final, optimized plan.

- `Executor`– The Executor employs multiple LLMs to perform computation and optimization tasks in parallel. Based on the optimal data selected by the Analyzer and Planner, these AI models work simultaneously to generate infrastructure mangement and feedback data.

- `Knowledge`– The Knowledge component uses an array of LLMs to manage data effectively. These models work in parallel to generate appropriate queries for the actual database, ensuring accurate and diverse data retrieval and manipulation strategies.

3.2   Implementation

3.2.1   Types of LLMs Used in CENTAURI

CENTAURI architecture allows for the integration of multiple LLM services through their respective APIs. To implement this functionality, CENTAURI can interface with several leading commercial LLM services that provide robust API support. Table 1 presents examples of potential AI vendors and their models that could be integrated into the CENTAURI system. In addition to commercial AI services, CENTAURI is designed to incorporate private AI models trained on diverse ranges of data. These private AI models can be customized to meet specific cybersecurity training needs and can process sensitive or proprietary information that may not be suitable for commercial AI services.

Vendor	Models
Google	Gemini 1.5 Flash, Gemini 1.5 Pro
OpenAI	GPT-4 Turbo, GPT-4o, GPT-4o mini
Anthropic	Claude 3 Sonnet, Claude 3 Opus, Claude 3.5 Sonnet

Table 1: List of LLM Vendors and their Models

3.2.2 CENTAURI-Infrastructure

CENTAURI-Infrastructure builds its cybersecurity training environment on a self-established OpenStack cluster using Python Openstack SDK and Ansible[3]. The tenant isolation feature of OpenStack allows multiple cybersecurity training environments to run in isolated environments, providing the advantage of applying various scenarios in parallel. Additionally, resources can be allocated selectively depending on the scenario and the participants, with infrastructure control features supported within limited resources.
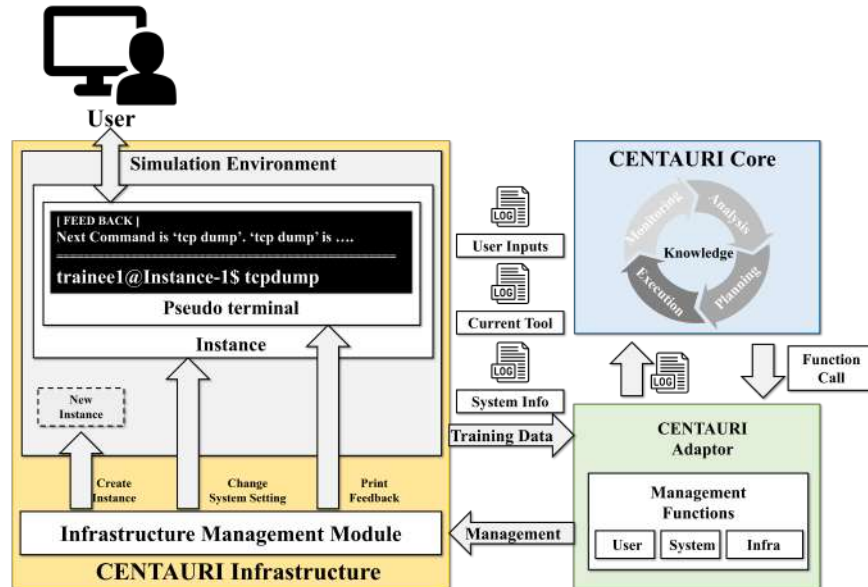

Figure 3: Detailed Configuration of CENTAURI Infrastructure

As shown in Figure 3, within the CENTAURI-Infrastructure, each instance and node is equipped with a pseudo Terminal that facilitates direct interaction between trainees and the training environment. This pseudo Terminal functions as a sophisticated monitoring and data collection interface. It captures and records in real-time all trainee-input commands, executed processes, and current system states. This continuous monitoring and data collection enable CENTAURI to perform detailed analysis of trainee behavior, track progress, and adapt the training scenario dynamically.

3.2.3   CENTAURI-Adapter

CENTAURI-Adapter predefine a specialized set of functions tailored for the cybersecurity training environment, enabling seamless integration with LLM. This function set simplifies communication with the OpenStack environment, minimizes token consumption, and facilitates parallel data collection and utilization. Specifically, these functions include core infrastructure management capabilities such as querying virtual machine states, creating networks, updating security group rules, and generating snapshots. These functionalities are implemented using the Python OpenStack SDK and Ansible within CENTAURI-Infrastructure. Furthermore, through a set of system command execution functions, CENTAURI-Adapter perform tasks such as collecting trainee activity logs, deploying training scenarios using Ansible, adjusting dynamic resources, and generating result reports in real time.

3.2.4   CENTAURI-Core

CENTAURI-Core is perform specific analysis and control functions, multiple LLM services. This computation are used as a training tutor for each CENTAURI-Core, which aims to achieve tasks such as "Infrastructure Analysis and Control", "Trainee Input Data Analysis", and "Real-Time Feedback Generation".

- `Initialization`– The initialization process begins with the selection of appropriate LLMs from the available API-Pool based on the specific requirements of each components of CETAURI-Core and the current training scenario. Following this selection, AI sessions are invoked, establishing connections with the chosen LLM services. The system then activates CENTAURI-Infrastructure, ensuring all necessary components and resources are available.

- `Trainee Input Data Analysis`– The trainee Input Data Analysis module monitors and analyzes trainee activities in real-time. It collects all trainee inputs and system interactions using a distributed stream processing system, and utilizes LLM analytical capabilities to identify trainee problem-solving patterns.

- `Real-Time Feedback Generation`– The Real-Time Feedback Generation module continuously analyzes trainee behavior and provides targeted support to achieve training objectives. By leveraging LLM, it performs real-time assessment of trainee actions within the cybersecurity training environment. This module interprets the trainee's problem-solving approaches, identifies areas for improvement, and generates instantaneous, context-aware hints and feedback. It utilizes NLP(Natural Language Processing) technologies to deliver clear, actionable guidance tailored to the trainee's current progress and learning style.

- `Infrastructure Analysis and Control`– The Infrastructure Analysis and Control module dynamically adjusts the training environment based on the trainee's skill level. It uses connected LLM services to perform multi-dimensional analysis of the trainee's abilities, and applies the optimal infrastructure configuration proposed by the AI by executing control functions through CENTAURI-Adapters, thereby automating the infrastructure deployment. This allows for immediate adjustments to the CENTAURI-Infrastructure environment in response to changing trainee needs or scenario requirements.

3.2.5   Message Protocol

The MAPE-K components within CENTAURI-Core perform a three-stage computational process for cyclic autonomous computing. During these operations, each component of the Core

engine uses a standardized message structure that includes execution states and result data from the MAPE-K loop operations. The message structure provides a consistent format for communication between components, as shown in Figure 4, ensuring efficient data transfer and processing throughout the system. During each component's operation process, LLM model sessions are dynamically allocated through communication with the API Pool. The allocated LLM models manage control flow through Function Call information provided during the inference request process.
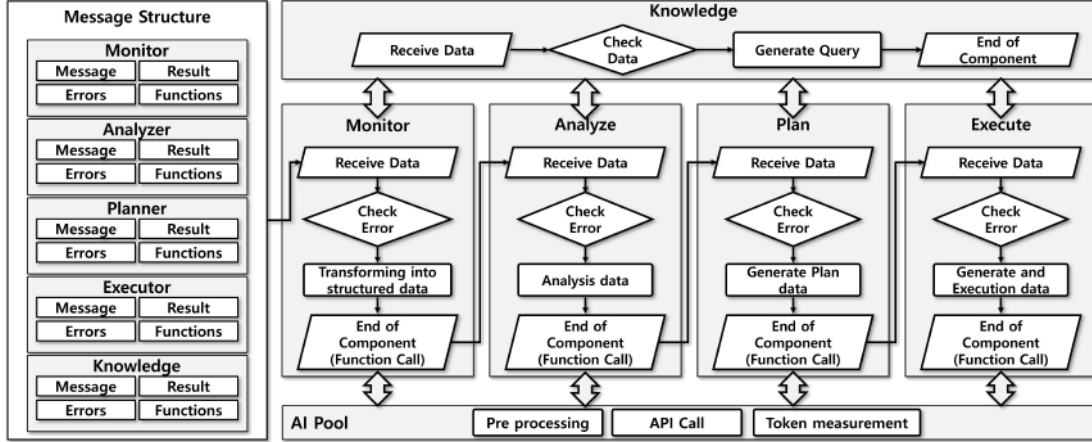

Figure 4: Message structure and MAPE-K workflow diagram in CENTAURI Core

The API Pool serves as the central hub in inter-component message processing. When LLM models complete their message processing and analysis at each stage, the messages are systematically passed to subsequent components following the MAPE-K loop procedure, as illustrated in Figure 4. These transmitted messages strictly adhere to the message structure protocol and contain essential metadata for processing status tracking. The implemented message protocol incorporates several key features essential for robust system operation. It utilizes a standardized message format across all component communications, supporting both synchronous and asynchronous processing capabilities. This structured message protocol enables CENTAURI to maintain efficient communication between components while ensuring reliable and traceable operations throughout the system.

4   Evaluation

This section discusses the experimental validation of CENTAURI based on predefined experimental environments and conditions. We evaluate the effectiveness of LLM interactions with trainees and demonstrate the practical feasibility of CENTAURI through comprehensive implementation analysis.

4.1   Experimental Environment

CENTAURI integrates commercial LLM models listed in 1, with each model accessed through standardized API communication protocols. API requests are processed asynchronously to ensure real-time processing efficiency, with each model generating consistent results using identi-
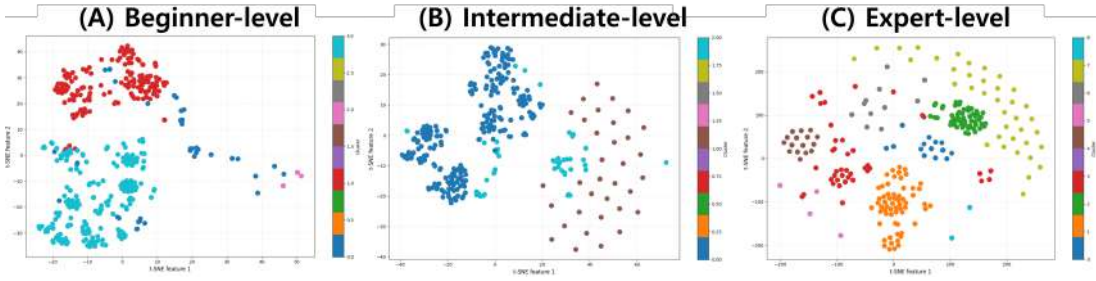
Figure 5: Clustering analysis of Data patterns across different skill levels.

cal prompts and data formats. The CENTAURI-Infrastructure is built on OpenStack Caracal, consisting of three compute nodes, one controller node, and one block node. The network infrastructure provides 10Gbps bandwidth to support real-time data processing and analysis requirements.

4.2　Performance Analysis and Trainee Behavior Patterns

This section validates the consistency of control and feedback data generated by CENTAURI when analyzing real-time trainee interactions and managing the training environment. We specifically analyze whether CENTAURI generates similar infrastructure control patterns and feedback responses when interacting with trainees of equivalent skill levels. For this analysis, trainee capabilities were classified into three levels (Beginner, Intermediate, and Expert), and we examined CENTAURI's generated responses and control actions for each level.

Text embedding-based clustering was performed to verify the similarity of CENTAURI's generated control and feedback data. Cluster quality was evaluated using metrics including silhouette score, inter-cluster distance, and intra-cluster distance. Figure 5 shows the embedding-based similarity analysis results of infrastructure control commands and feedback patterns generated by CENTAURI for each trainee capability level.

Analysis of beginner-level trainees (Figure 5(A)) shows that CENTAURI's responses comprised 466 control action data points grouped into 4 clusters. The larger inter-cluster distance (0.936) compared to the intra-cluster distance (0.696) indicates that CENTAURI maintains distinct control patterns when managing beginner-level training scenarios.

For intermediate-level trainees (Figure 5(B)), CENTAURI generated 333 control action data points that formed 3 clusters. The distribution shows one dominant cluster (69.4%) with two smaller clusters (15.6%, 15.0%), indicating that CENTAURI maintains a primary control strategy while providing specialized adaptations for specific training scenarios at this level.

In the case of expert-level trainees (Figure 5(C)), CENTAURI generated 810 control action data points distributed across 9 clusters. This group demonstrated the highest clustering quality scores with relatively even cluster size distribution, suggesting that CENTAURI implements more diverse control strategies for expert trainees, effectively adapting its responses to match their advanced capabilities and varied problem-solving approaches.

Outlier data points not included in the main clusters were observed across all capability levels. Upon analysis, these outliers appear to stem from several inherent limitations of LLMs. The first significant limitation is the bias present in LLM models, which can lead to inaccurate judgments in data processing. Another critical limitation is the hallucination phenomena, where LLMs generate unrealistic reasoning that deviates from expected patterns. Additionally, error

propagation in complex analysis chains contributes to the generation of outlier data points. This is particularly evident in the beginner-level data, where scattered data points appear, and in intermediate-level data, where portions of small clusters show anomalous patterns. These abnormal data patterns can be attributed directly to the current limitations of LLM technology. However, these limitations are not permanent obstacles, as they are expected to be addressed and resolved through ongoing research and future advancements in LLM technology.

4.3   Technical Limitations and Challenges

Outlier data points not included in the main clusters were observed across all capability levels. Upon detailed analysis, these outliers were found to originate from several inherent limitations of LLMs. First, the bias present in LLM models can lead to inaccurate judgments during data processing and analysis phases. Second, the hallucination phenomena in LLMs occasionally results in generating unrealistic reasoning that deviates from expected control patterns. Additionally, error propagation in complex analysis chains contributes to the generation of outlier data points in CENTAURI's responses. This limitation is particularly evident in the control patterns for beginner-level interactions, where scattered data points appear, and in intermediate-level responses, where portions of small clusters show anomalous patterns. While these abnormal data patterns can be attributed directly to the current limitations of LLM technology, they are not permanent obstacles.

5   Discussion

5.1   Privacy and Ethical Considerations

The development and operation of CENTAURI require careful consideration of trainee privacy protection and ethical aspects. The platform's ability to monitor and analyze trainee behaviors in cybersecurity training environments raises significant privacy concerns. trainee interactions, including command patterns and problem-solving approaches, can reveal individual characteristics and capabilities that require protection.

CENTAURI addresses these privacy concerns through its cloud-based virtualization approach. By collecting data exclusively within isolated virtual instances rather than trainees' local environments, the system maintains a clear boundary between training activities and personal computing spaces. This approach effectively prevents the collection of personal activities outside the training context while ensuring comprehensive capture of relevant training data.

The system's cloud-based infrastructure enables robust implementation of security controls through systematic policies. Centralized data collection and storage facilitate consistent application of access control and encryption protocols across all training sessions.

5.2   Further work

While CENTAURI proposes an innovative approach to cybersecurity training through LLM integration, several technical challenges require further development. The primary limitations stem from current LLM capabilities, including response consistency issues in complex scenarios and occasional deviations in behavioral analysis. These technical constraints impact the system's ability to maintain consistent training experiences across different trainee skill levels.

Future development will focus on enhancing CENTAURI's core capabilities through several key improvements. First, the integration of advanced LLM technologies and development of

specialized cybersecurity training models will improve analysis accuracy and response consistency. Second, enhanced real-time processing capabilities will enable more sophisticated feedback mechanisms and dynamic scenario adaptation. These improvements will require significant advances in both underlying technology and methodological approaches. Ongoing research will concentrate on developing more efficient reasoning methods leveraging emerging LLM capabilities and optimized data structures.

6   Conclusion

This paper presents CENTAURI, a cloud-based cybersecurity training platform powered by LLM. By integrating multiple LLMs, CENTAURI offers a dynamic, personalized training experience, enhancing the learning process for cybersecurity professionals while improving the efficiency of infrastructure automation and resource management.

The key contributions of CENTAURI include the integration of multiple AI models for enhanced analysis capabilities, real-time behavioral assessment, automated infrastructure control for efficient resource management, and continuous context-aware feedback generation. Our experimental results demonstrate that CENTAURI maintains consistent control patterns across different trainee skill levels, with clustering analysis revealing structured adaptation strategies for varying expertise levels.

As cyber threats continue to evolve in complexity and scale, platforms like CENTAURI will play an increasingly crucial role in cybersecurity education. While current technical limitations exist, particularly in LLM response consistency and complex scenario analysis, ongoing advancements in AI technology are expected to address these challenges. Future research will focus on enhancing the platform's capabilities through improved AI model integration, advanced privacy-preserving techniques, and more sophisticated training scenario generation.

7   Acknowledgments

References

[1] Robert G Abbott, Jonathan T McClain, Benjamin Robert Anderson, Kevin S Nauer, Austin Ray Silva, and James C Forsythe. Automated performance assessment in cyber training exercises. Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2015.

[2] Vishwanath Akuthota, Raghunandan Kasula, Sabiha Tasnim Sumona, Masud Mohiuddin, Md Tanzim Reza, and Md Mizanur Rahman. Vulnerability detection and monitoring using llm. In *2023 IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*, pages 309–314. IEEE, 2023.

[3] Narjes Bessghaier, Mohammed Sayagh, Ali Ouni, and Mohamed Wiem Mkaouer. What constitutes the deployment and runtime configuration system? an empirical study on openstack projects. *ACM Transactions on Software Engineering and Methodology*, 33(1):1–37, 2023.

[4] Phan The Duy, Hien Do Hoang, Nghi Hoang Khoa, Van-Hau Pham, et al. A case study for evaluating learners' behaviors from online cybersecurity training platform on digital forensics subject. In *2022 International Conference on Advanced Technologies for Communications (ATC)*, pages 251–256. IEEE, 2022.

[5] The European Union Agency for Cybersecurity(ENISA). Best practices for cyber crisis management, 2024. Accessed: 2024-09-20.

[6] Magdalena Glas, Manfred Vielberth, and Guenther Pernul. Train as you fight: evaluating authentic cybersecurity training in cyber ranges. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2023.

[7] Philip Huff, Sandra Leiterman, and Jan P Springer. Cyber arena: an open-source solution for scalable cybersecurity labs in the cloud. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, pages 221–227, 2023.

[8] Sunjae Kwon, Sungu Lee, Taehyoun Kim, Duksan Ryu, and Jongmoon Baik. Exploring llm-based automated repairing of ansible script in edge-cloud infrastructures. *Journal of Web Engineering*, 22(6):889–912, 2023.

[9] Maria Leitner, Maximilian Frank, Wolfgang Hotwagner, Gregor Langner, Oliver Maurhart, Timea Pahi, Lenhard Reuter, Florian Skopik, Paul Smith, and Manuel Warum. Ait cyber range: flexible cyber security environment for exercises, training and research. In *Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference*, pages 1–6, 2020.

[10] Sten Mäses, Kaie Maennel, and Agnė Brilingaitė. Trends and challenges for balanced scoring in cybersecurity exercises: A case study on the example of locked shields. In *Frontiers in Education*, volume 7, page 958405. Frontiers, 2022.

[11] Takeru Naito, Rei Watanabe, and Takuho Mitsunaga. Llm-based attack scenarios generator with it asset management and vulnerability information. In *2023 6th International Conference on Signal Processing and Information Security (ICSPIS)*, pages 99–103. IEEE, 2023.

[12] Nathalia Nascimento, Paulo Alencar, and Donald Cowan. Gpt-in-the-loop: Supporting adaptation in multiagent systems. In *2023 IEEE International Conference on Big Data (BigData)*, pages 4674–4683. IEEE, 2023.

[13] National Institute of Standards and Technolog(NIST). The cyber range: A guide., 2023. Accessed: 2024-09-20.

[14] V Švábenskỳ. *Automated feedback for cybersecurity training*. PhD thesis, Doctoral thesis, Masaryk University, 2022.[Online]. Available: https://is . . . , 2022.

[15] Csaba Virág, Jakub Čegan, Tomáš Lieskovan, and Matteo Merialdo. The current state of the art and future of european cyber range ecosystem. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 390–395. IEEE, 2021.

[16] Daniel Votipka, Eric Zhang, and Michelle L Mazurek. Hacked: A pedagogical analysis of online vulnerability discovery exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1268–1285. IEEE, 2021.