An IT/OT Converged Cyber Range Framework Supporting Ensemble of Large Multimodal Models-Human Teaming and RAG Capability for Bigdata Information Retrieval – 6G Perspective

M. Abdur Rahman
Cyber Security and Forensic Computing Department
University of Prince Mugrin
Medina, Saudi Arabia
m.arahman@upm.edu.sa

M. Saiful Islam
UoL Worldwide
University of London
London, United Kingdom
msi79@student.london.ac.uk

M. Repon Islam
Department of Computer Science and Engineering
Khulna University of Engineering & Technology
Khulna, Bangladesh
repon@cse.kuet.ac.bd

M. Shamim Hossain
Department of Software Engineering
King Saud University
Riyadh, Saudi Arabia
mshossain@ksu.edu.sa

Selwa Al-Hazzaa
Digital Innovation Sector
King Abdulaziz City for Science and Technology (KACST)
Riyadh, Saudi Arabia
salhazzaa@kacst.gov.sa

GLOBECOM 2024 - 2024 IEEE Global Communications Conference | 979-8-3503-5125-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/GLOBECOM52923.2024.10901738

***Abstract*— In IT/OT converged enterprise networks, the management of multimodal big data has surpassed human capabilities, presenting critical challenges in business decision-making. This paper introduces an innovative IT/OT Converged Cyber Range Framework, leveraging the power of 6G technology alongside an ensemble of large multimodal models (LMMs) equipped with Retrieval Augmented Generation (RAG) capabilities. Our proposed framework excels at parsing and retrieving information from diverse and massive multimodal datasets in near real-time, driven by the integration of LMMs and human interactions in natural language. The framework's advanced configuration with RAG achieved top performance with an average score of 80.5 across key metrics, including an 86 in answer relevancy and an 88 in faithfulness, while effectively reducing hallucinations to a score of 26. By combining 6G's connectivity with advanced LMM capabilities, we significantly improve the efficiency of automated big data processing and information retrieval, thereby transforming decision-making processes in IT/OT environments. The implementation of our framework, validated through real-life big data sources, and the encouraging test results showcase its effectiveness and transformative potential in managing and utilizing big data far beyond traditional human capabilities.**

***Keywords*—*Large Multimodal Models (LMMs), Multimedia Bigdata, Retrieval Augmented Generation (RAG), IT/OT Converged Network, Human-LMM Teaming, 6G Technology.*

I. Introduction

The imminent rollout of 6G technology promises transformative changes in telecommunications, characterized by ultra-high speeds and robust connectivity. This next-generation network is not merely an enhancement in communication speed; it fundamentally revolutionizes how data is processed and shared among various entities [1]. By enabling real-time data exchange and automated network management through advanced artificial intelligence, 6G paves the way for more dynamic and integrated digital ecosystems [2]. Such capabilities are crucial in supporting the extensive data interactions required in modern IT/OT environments.

As industries increasingly rely on digitized operations, the volume of data generated within IT/OT converged environments has grown exponentially. This surge in data encompasses various formats and is often too vast for traditional processing methods to handle efficiently. Here, the high-speed, real-time communication facilitated by 6G becomes invaluable [3]. The technology's ability to rapidly process and retrieve large datasets can significantly enhance functions such as data insights extraction, reporting, and backup services across multiple industry verticals [2].

To further tackle the challenges of diverse data types, Large Multimodal Generative AI (LMM) has emerged as a pivotal technology [4]. LMMs adeptly analyze and synthesize information from disparate sources — including text, images, audio, and video — enabling a comprehensive and nuanced understanding of big data [4]. These AI models are particularly effective when paired with the capabilities of 6G, as they require the kind of bandwidth and low latency that 6G networks provide to operate optimally and deliver near real-time insights [5]. The convergence of 6G and LMM technologies marks a critical advancement in network and AI capabilities [6]. This integration allows users to interact with the network in natural language, greatly simplifying the management of complex data sets and enhancing user accessibility.

Moreover, the combination of 6G's swift data transmission with LMM's robust processing power enables simultaneous retrieval and analysis of multi-media data, facilitating immediate sharing and utilization of insights [5].

Building upon the high-speed capabilities of 6G, the development of Large Multimodal Models (LMM) within IT/OT converged networks becomes not only feasible but also highly efficient. The substantial bandwidth provided by 6G is essential for handling the enormous volumes of multimedia big data, as depicted in the shared diagram.

Figure 1 illustrates the complex ecosystem where physical systems and virtual systems are interconnected through an AI-enhanced 6G network [7]. The variety of enterprise big datasets—ranging from massive files of multiple media types, configuration and asset datasets to more dynamic timeseries and network traffic datasets—contributes to a comprehensive Big Dataset Collection. This collection is pivotal for the continuous learning and evolution of LMMs [8]. The LMM, acts as the human natural language interface, processing diverse data types, including media, graph, and endpoint detection and response (EDR) datasets.

The RAG capabilities of these models can leverage the high throughput and low latency of 6G networks to rapidly assimilate and analyze new data, thereby supporting the decision-making processes inherent in the IT/OT sectors [9].

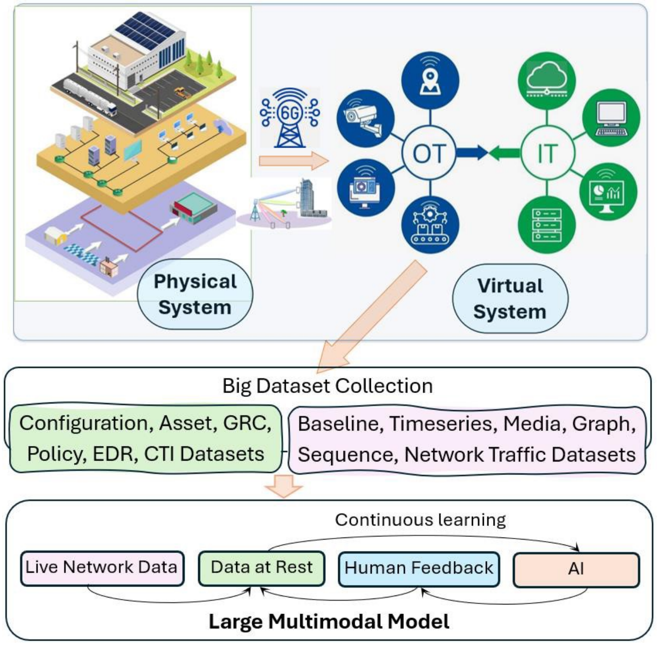


Figure 1: Salient components of big data sources within an IT/OT converged network assisted with large multimodal models.

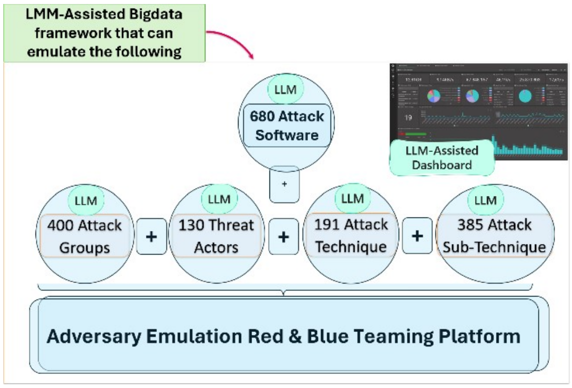
This seamless flow of information, powered by 6G, ensures that LMMs are consistently fed with the most up-to-date data, fostering an environment of continuous learning and real-time insight generation. It underscores the necessity for such advanced models to interpret and act upon a vast array of data types instantaneously, a process that is made viable by the advanced communication infrastructure provided by 6G technology [1].

In advancing the state-of-the-art in IT/OT security and efficiency, cyber range is pivotal, which is a simulation environment designed to emulate an IT/OT converged network, complete with necessary virtual machines (VMs) and network topologies that mirror real-world big data scenarios and 6G communication paradigms [10]. Within this emulated environment, the cyber range facilitates the generation of diverse big data, reflecting true operational data flows and interactions.

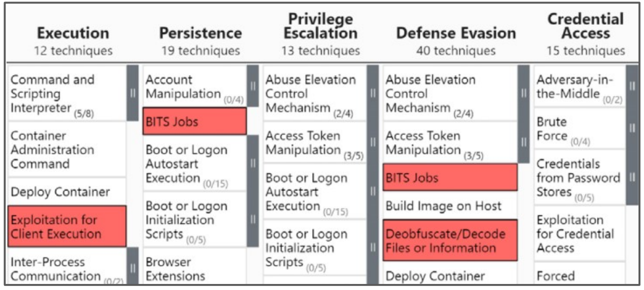
Moreover, the cyber range serves as an essential testbed for modeling big data generation, utilization, and the critical process of insight extraction [10]. This encompasses the simulation of unauthorized access scenarios and adversarial attacks targeting big data repositories, which are increasingly common in the digital age [11]. By incorporating red and blue teaming exercises within the cyber range, we can realistically replicate attack and defense dynamics. Adversarial red teams are tasked with launching sophisticated cyberattacks on big data sources, while blue teams, empowered by LMM technologies, work to rapidly glean insights from the evolving situation to identify and mitigate these threats [12].

However, realizing such system would require identifying the critical challenges that this paper will address in the realm of LMM-supported 6G networks and massive multimodal data insight retrieval. A foremost challenge lies in scaling Large Multimodal Models (LMMs) to operate within the expansive realms of 6G networks. The substantial bandwidth and reduced latency promised by 6G necessitate LMMs that can not only process larger volumes of data but also do so with unprecedented speed and efficiency [12]. This scalability is essential for real-time big data analytics and the resultant need for LMMs to adapt their architectures to these hyper-accelerated environments without compromising accuracy or performance [4].

Securing LMM-enabled 6G networks presents a novel set of security challenges. The integration of AI into high-speed networks opens new attack vectors for cyber threats, which exploit the complex interplay between high-throughput data pipelines and AI-driven decision-making. The vast repositories of big data in enterprise systems present an array of security vulnerabilities, particularly susceptible to sophisticated cyber threats as depicted in **Figure 2 (a)**. The challenge extends beyond the mere safeguarding of data; it encompasses the constant monitoring for and defending against adversarial attacks, which are becoming increasingly complex. Adversaries are now leveraging LMMs to craft attacks that align with the MITRE ATT&CK framework, utilizing an array of Tactics, Techniques, and Procedures (TTPs) to target IT/OT systems (see **Figure 2(b)**).



(a)



Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques
Command and Scripting Interpreter (5/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (2/4)	Abuse Elevation Control Mechanism (2/4)	Adversary-in-the-Middle (0/2)
Container Administration Command	BITS Jobs	Access Token Manipulation (3/5)	Access Token Manipulation (3/5)	Brute Force (0/4)
Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs	Credentials from Password Stores (0/5)
Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access
Inter-Process Communication (0/2)	Browser Extensions		Deobfuscate/Decode Files or Information	Forced
			Deploy Container	

(b)

Figure 2: Generating network traffic using LMM and defensive big data information retrieval architecture through adversarial examples.

The challenges of modern cybersecurity and big data management necessitate the integration of Large Multimodal Models (LMMs) within a 6G-enabled cyber range. LMMs are crucial for both the emulation of sophisticated cyber threats, through a deep understanding of MITRE ATT&CK tactics, techniques, and procedures (TTPs), and the development of dynamic defenses. Each of these challenges is intricately connected to the core functionalities of an LMM-augmented 6G framework and calls for innovative research and development.

The subsequent sections of this paper will delve into the solutions and methodologies proposed to address these complex issues, paving the way for a new dimension in IT/OT network operations and security.

To attain this, this paper makes the following contributions:

- We introduce a scalable LMM-assisted cyber range framework optimized for 6G network environments, capable of real-time, multimodal big data processing and insight generation.
- Our framework presents an innovative integration of LMMs for proactive and automated insight extraction from massive enterprise data sources, reducing reliance on manual query processing.
- We detail the development of a novel LMM-based defensive mechanism, tailored to recognize and mitigate sophisticated adversarial attacks aligned with MITRE ATT&CK TTPs within IT/OT environments.
- The paper demonstrates the effective use of LMM-enhanced red and blue teaming exercises within a cyber range, showcasing enhanced detection and response capabilities against complex cyber threats on big data systems.

The remainder of this paper is organized as follows: Section II describes the methodology, detailing the architecture of the proposed LMM-assisted cyber range framework and its integration within 6G networks. Section III elaborates on the implementation of the framework, including the configuration of LMMs for multimodal data interaction and the setup of the cyber range for emulation exercises. Section IV presents a rigorous analysis of the results from our testbed, highlighting the efficiency of real-time data processing and the efficacy of our novel LMM-based defensive mechanisms. Finally, Section V concludes the paper with a summary of our contributions and a discussion on the future work prompted by our research.

II. SYSTEM DESIGN AND METHODOLOGY

A. Design of the Range Environment:

The cyber range's network topology is depicted in Figure 3, which is meticulously crafted to emulate a comprehensive IT/OT converged environment. The topology integrates a variety of virtual machines (VMs), including dedicated LMM VMs for analytics, big data generation, and storage VMs, as well as attacker and defender VMs for red and blue teaming exercises. This setup not only allows for a controlled emulation of enterprise and industrial network segments but also ensures that each node can simulate specific aspects of a 6G-enabled communication ecosystem. Critical to this environment is the 6G VM, which serves as a gateway for high-speed data processing.

Central to the cyber range are the LMM VMs which, as shown in the figures, are strategically placed within both IT and OT VLANs to reflect their role in processing and analyzing data from various sources. These VMs are equipped with cutting-edge analytical tools, facilitating the extraction of insights from multimodal data in real-time, mirroring the high throughput anticipated in 6G networks. Similarly, the inclusion of VMs for adversarial emulation and security operations—like the Kali Linux VM for red team attacks and the Security Onion VM for blue team defenses—provides the necessary components to rigorously test the resilience of big data systems against sophisticated cyber threats.

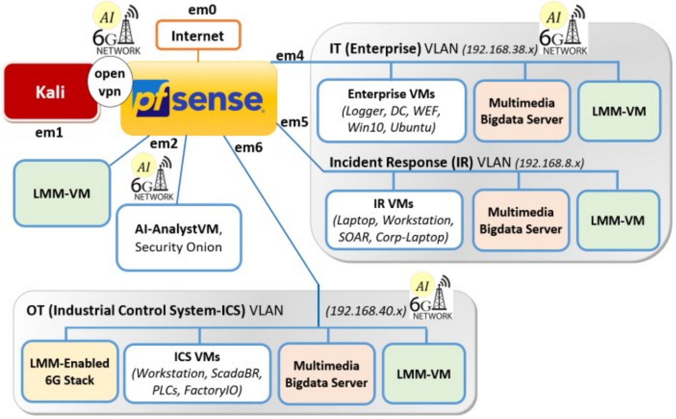

AI
6G NETWORK
em0
Internet
Kali
open vpn
pfsense
em1
em2
em4
em5
em6
LMM-VM
AI
6G NETWORK
AI-AnalystVM, Security Onion
IT (Enterprise) VLAN (192.168.38.x)
AI
6G NETWORK
Enterprise VMs (Logger, DC, WEF, Win10, Ubuntu)
Multimedia Bigdata Server
LMM-VM
Incident Response (IR) VLAN (192.168.8.x)
IR VMs (Laptop, Workstation, SOAR, Corp-Laptop)
Multimedia Bigdata Server
LMM-VM
OT (Industrial Control System-ICS) VLAN
(192.168.40.x)
AI
6G NETWORK
LMM-Enabled 6G Stack
ICS VMs (Workstation, ScadaBR, PLCs, FactoryIO)
Multimedia Bigdata Server
LMM-VM

Figure 3: Network topology of the proposed cyber range emulating bigdata sources, attacker VMs, defender VMs, bigdata sources, IT/OT converged network, and large multimodal models.

The comprehensive network topology and VM configuration support a wide range of scenarios for both routine operations and cybersecurity drills. Experimentation with big data information retrieval and insight generation is conducted in an environment that accurately reflects the speed and complexity of a real-world 6G network.

B. Design of the 6G Testbed Environment:

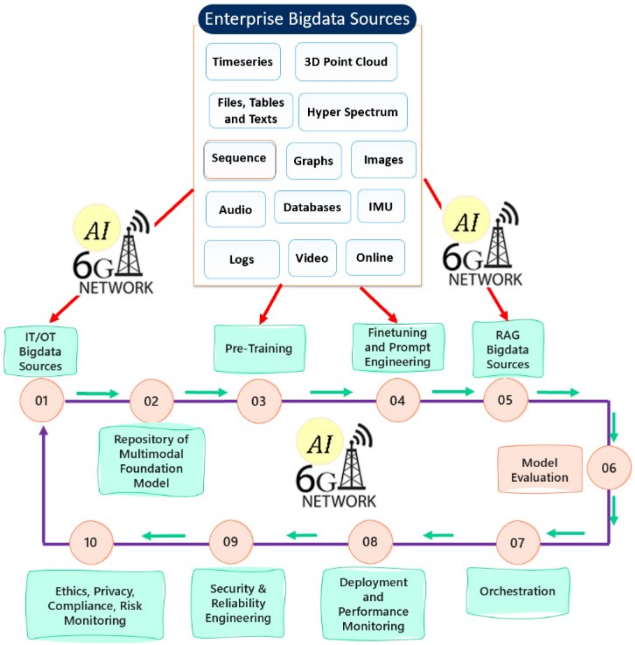


Figure 4: Lifecycle of the proposed bigdata information retrieval system through 6G and LMM stack.

Our proposed framework includes an emulated 6G testbed. The automation platform, Ansible, streamlines the configuration and deployment of the network, ensuring that every component can be dynamically adjusted to meet the demands of various data-intensive scenarios. Virtual Machine (VM) deployment via VirtualBox provides the necessary isolation and dedicated resources for distinct network functions, while Docker containers enable lightweight and scalable service instantiation. These components form the backbone of the emulated 6G environment, offering an adaptable testbed for the deployment of LMM-driven big data analytics and cybersecurity protocols.

The emulation is further refined by incorporating a network architecture, ensuring a realistic simulation of 6G communication. Docker containers encapsulate the core network functions—User Equipment (UE), evolved NodeB (eNB), and 5G Core (5GC) elements (AMF, SMF, HSS, PCRF, UPF)—mirroring the functional deployments found in modern 5G architectures and setting the stage for advanced 6G R&D.

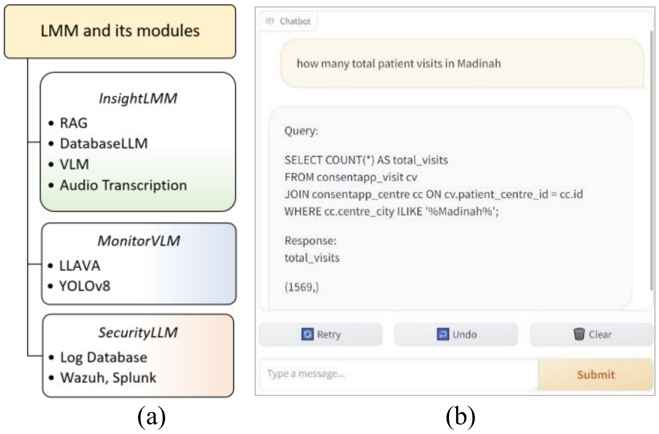
C. Design of the LMM Stack:

The proposed LMM stack, as illustrated in **Figure 4**, is an integral component of our framework, embodying the lifecycle of big data information retrieval through a 6G and AI-enabled network. Beginning with diverse IT/OT big data sources, such as timeseries, multimedia files, and complex databases, the data flows into a pre-training stage where foundational models are tailored to understand and process this heterogeneous information. As we progress to finetuning and prompt engineering, the LMM stack is refined to interact specifically with the big data relevant to enterprise contexts, applying RAG to hone in on valuable insights. This process is critical for transforming the raw big data into actionable intelligence, enabling the system to not only retrieve information but also predict and suggest based on the latest data inputs. The subsequent orchestration phase ensures that these insights are seamlessly integrated, with the 6G network facilitating real-time communication of the LMM outputs.

The lifecycle concludes with rigorous model evaluation, where the output is assessed for accuracy, relevance, and timeliness. This evaluation is followed by ethics, privacy, and compliance, ensuring that the system adheres to the highest standards of data governance. Security and reliability engineering is woven throughout the stack, safeguarding the system against cyber threats while maintaining peak operational performance.

III. IMPLEMENTATION

Our cyber range infrastructure is powered by state-of-the-art components optimized for LMM and big data challenges. It harnesses the computational power of 4 NVIDIA H100 GPUs, necessary for training models like LLAMA2, Mistral, and Zephyr. The system's 2TB DDR4 ECC RAM is essential for handling extensive in-memory operations during model training, while a substantial 10TB of NVMe SSD storage enables swift read/write operations for managing voluminous datasets and model checkpoints and efficiently distribute the workload for various language and vision tasks executed by models such as LLAVA, Stable Diffusion, DALL-E, DINO, SAM, and Yolov8.



how many total patient visits in Madinah

```
Query:

SELECT COUNT(*) AS total_visits
FROM consentapp_visit cv
JOIN consentapp_centre cc ON cv.patient_centre_id = cc.id
WHERE cc.centre_city ILIKE '%Madinah%';

Response:
total_visits

(1569,)
```

(a) (b)

Figure 5: (a) the ensemble of large multi-modal models within the range of VMs, and (b) a running database insight LLM where users can query any database in natural languages.

A. Implemented Model Details (see **Figure 5(a)**):

- InsightLMM (Mistral, Zephyr, Mixtral 8x7B) finetuned with the organization's domain-specific training data, connected with the below modules:
  - RAG from multiple source types
  - DatabaseLLM (SQLCoder) connected with the organization’s real-time database to get important insights on-demand (see **Figure 5(b)**).
  - Vision Language Model (VLM) (LLAVA) for understanding visual data along with object detection and face recognition model
  - Audio transcription (SeamlessM4T), meeting summarization (Mistral) and storing of summarized notes
- MonitorVLM (LLAVA) for real-time explainable and automated monitoring of employee, person, and various emergency surveillance conditions
- SecurityLLM finetuned with security datasets used for analyzing millions of systems-generated logs along with Wazuh, Splunk, etc. for explaining security issues with multiple threat levels.

B. Implemented Scenario – Attack on Bigdata:

To showcase the novel idea as a PoC, we have emulated a railway IT/OT converged network as a set of VMs. Within the cyber range, an intricate emulation of a railway IT/OT system has been constructed, capturing the complexities of a real-world scenario where IT networks manage corporate functions, while OT networks handle supervisory control and data acquisition (SCADA) systems critical to railway operations. The corporate network hosts IT management computers and servers, essential for everyday business processes, whereas the OT network, comprising SCADA and production networks, directly interfaces with the physical railway infrastructure, monitoring train movements and station controls. This emulation serves as a dynamic backdrop for testing the resilience and efficiency of big data processing and retrieval mechanisms under various operational and attack scenarios.

Our cyber range's capabilities were rigorously tested through a series of red teaming exercises, simulating sophisticated cyberattacks targeting the railway's IT and OT networks. The first type of attack was a phishing and backdoor trojan campaign. The red team sought entry through social engineering, delivering malware that could bypass firewalls and penetrate the corporate network to compromise critical servers. The second scenario depicted a more direct attack on the OT—malware ARP attacks using tools like Ettercap for MiTM (Man-in-the-Middle) exploits, aiming to disrupt the real-time monitoring and control of train movements by blocking or altering PLC (Programmable Logic Controller) communications.

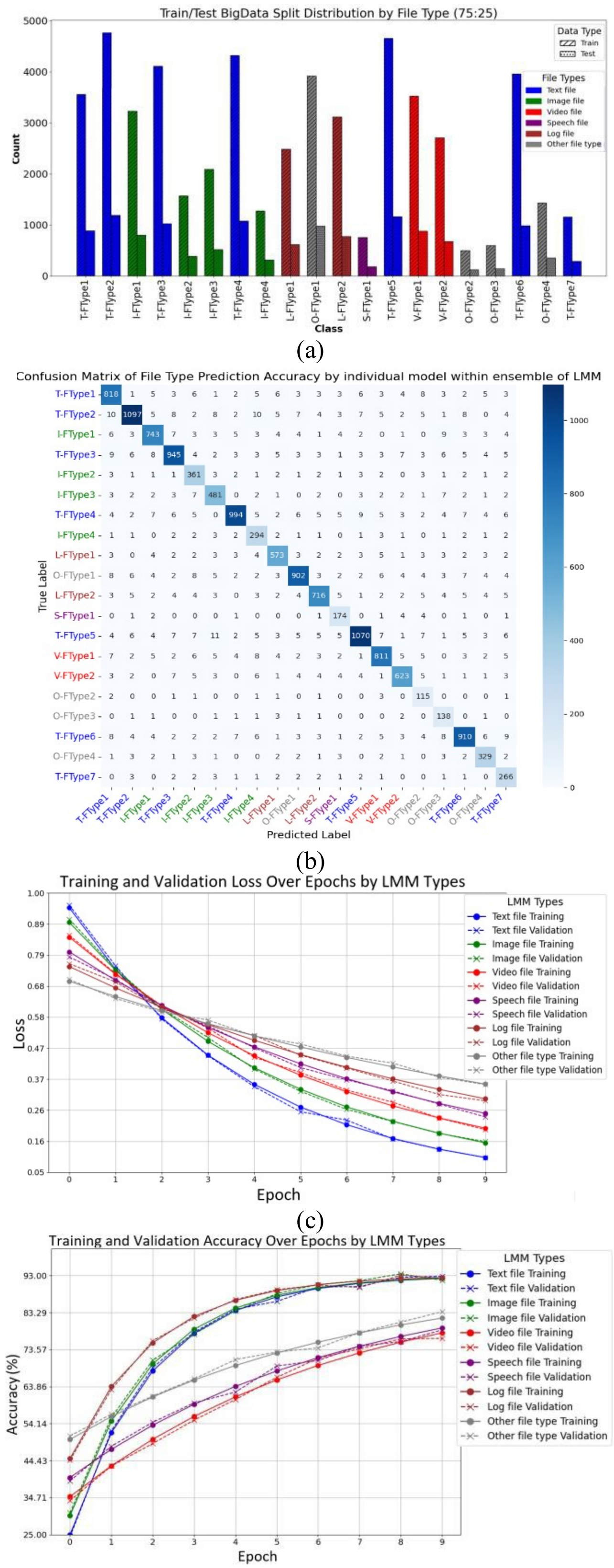
We also emulated false data/command injection attacks in which the red team injected illicit commands to manipulate train control systems, potentially leading to derailments or collisions. These attacks were characterized by their stealth and precision, altering Modbus communications to create false readings and responses in the PLCs. Finally, DDoS (Distributed Denial of Service) attacks tested the resilience of the network's communication channels.

C. Implemented Scenario – Bigdata Defense:

As for the defense LMMs, we have implemented and ensembled/assimilated a set of large multi-modal models as shown in **Figure 5 (b)**. InsightLMM and RAG are used in the early detection of phishing and backdoor attacks. MonitorVLM and YOLOv8 are used for real-time surveillance of ARP spoofing and false command injections while SecurityLMM is used in guarding against DDoS and false data injection. automated tagging of big data based on the security events is performed by SecurityLMM and MonitorVLM in automated surveillance mode.

IV. TEST RESULTS

To validate the system, we have captured two types of results: the training, test, and validation results of the multiple types of models followed by a performance comparison of a text-based LLM model with base, finetuning, and a combination of RAG + finetuning. The results, as illustrated in **Figure 6(a)**, depict the train/test distribution across various big data files and model types, showcasing the comprehensive nature of our LMM's big data processing capabilities. The variety in file types, from text to logs, mirrors the multimodal nature of data in IT/OT systems, ensuring that the LMM can handle the diverse data streams typical in railway network cybersecurity. The confusion matrix shown in **Figure 6(b)** presents the precision of file content prediction by individual models. **Figures 6(c)** and **(d)** shows LMM's performance in terms of loss and an increase in accuracy over epochs for both the training and validation phases. In the second phase of system testing, which is shown in **Figure 7**, we evaluate the performance variations across three distinct configurations of language processing models: the Base Model (Mistral 7B), a finetuned version, and an advanced finetuned variant equipped with Retrieval-Augmented Generation (RAG). We have used our own curated IT/OT converged cyber security-related dataset developed for this research. Given a total dataset of 233 instances, we selectively employed 100 data points for our testing procedure.



(a)

(b)

(c)

(d)

Figure 6: (a) Train/test distribution samples across different big data file types (b) Confusion matrix showing file type prediction accuracy of the LMM models, (c-d) training and validation loss and accuracy respectively.

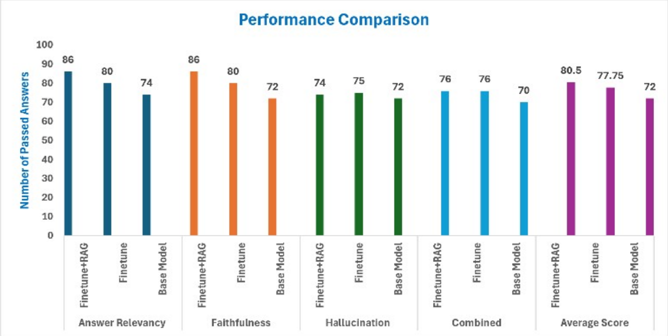


Figure 7: Performance comparison of LLM model based on base model, finetuning, and combination of RAG+finetuning.

The evaluation framework was constituted by three rigorous metrics: *answer relevancy metric*, *faithfulness metric*, and *hallucination metric*, establishing a comprehensive metric suite designed to holistically assess model performance. The predetermined benchmarks for satisfactory performance included a score of at least 0.5 for relevancy, and faithfulness metrics and a maximum allowable score of less than 0.3 for the hallucination metric to pass.

Our findings revealed that, averaged across all metrics, the finetune + RAG configuration is found to be the top-performing model, achieving an overall score of 80.5. This was followed by the finetuned model and the Base Model, with average scores of 77.75 and 72, respectively.

A more granular into individual metric performances uncovered that the finetune + RAG model demonstrated superior performance in enhancing answer relevancy and controlling hallucination with scores of 86 and 26 in the hallucination metric, indicative of a significant reduction in generated content that diverges from the ground truth. The finetune + RAG model also achieved an impressive 88 in faithfulness metric, affirming its ability to adhere closely to factual accuracy.

On the contrary, the finetuned model without RAG exhibited a decreased yet robust performance with 25 in hallucination, and notably, equal scores of 80 in both answer relevancy and faithfulness, maintaining a steady adherence to factual representation alongside a controlled level of hallucination. The foundational architecture, underperformed relative to its enhanced counterparts with 74 in answer relevancy, 72 in faithfulness, and marginally passing the hallucination metric with a score of 28.

V. CONCLUSION AND FUTURE DIRECTIONS

This paper has presented a comprehensive cyber range framework, leveraging the synergy between Large Multimodal Models (LMM) and the emerging 6G technology, aimed at enhancing big data processing and cybersecurity within IT/OT converged networks. We have demonstrated the integration and implementation of a scalable LMM-assisted framework, optimizing it for the bandwidth and low-latency environment that 6G networks promise. Through rigorous experimentation and validation exercises, we have shown that our framework is capable of effectively detecting, analyzing big data, and responding to sophisticated cyber threats in real time.

Looking ahead, the potential for expanding upon this framework is promising. Our future research will aim to explore the integration of even more sophisticated AI techniques, such as unsupervised learning algorithms that could further enhance the autonomous detection and mitigation of cyber threats. Additionally, the scalability of LMMs will be examined in the context of an expanding 6G infrastructure, with a focus on edge computing and the Internet of Things (IoT), where devices and sensors provide a plethora of data sources for LMM analysis.

REFERENCES

[1] Z. Zhang et al., “6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies,” IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 28–41, Sep. 2019, doi: 10.1109/MVT.2019.2921208.

[2] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, “Toward 6G Networks: Use Cases and Technologies,” IEEE Communications Magazine, vol. 58, no. 3, pp. 55–61, Mar. 2020, doi: 10.1109/MCOM.001.1900411.

[3] MA. Rahman and MS. Hossain, “A Deep Learning Assisted Software Defined Security Architecture for 6G Wireless Networks: IIoT Perspective,” IEEE Wirel Commun, vol. 29, no. 2, pp. 52–59, Apr. 2022, doi: 10.1109/MWC.006.2100438.

[4] J. Wu, W. Gan, Z. Chen, S. Wan, and P. S. Yu, “Multimodal Large Language Models: A Survey,” in 2023 IEEE International Conference on Big Data (BigData), IEEE, Dec. 2023, pp. 2247–2256. doi: 10.1109/BigData59044.2023.10386743.

[5] M. Xu et al., “When Large Language Model Agents Meet 6G Networks: Perception, Grounding, and Alignment,” Jan. 2024.

[6] B. Rong and H. Rutagemwa, “Leveraging Large Language Models for Intelligent Control of 6G Integrated TN-NTN with IoT Service,” IEEE Netw, pp. 1–1, 2024, doi: 10.1109/MNET.2024.3384013.

[7] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, “Artificial-Intelligence-Enabled Intelligent 6G Networks,” IEEE Netw, vol. 34, no. 6, pp. 272–280, Nov. 2020, doi: 10.1109/MNET.011.2000195.

[8] Y. Chang et al., “A Survey on Evaluation of Large Language Models,” ACM Trans Intell Syst Technol, vol. 15, no. 3, pp. 1–45, Jun. 2024, doi: 10.1145/3641289.

[9] Z. Feng, X. Feng, D. Zhao, M. Yang, and B. Qin, “Retrieval-Generation Synergy Augmented Large Language Models,” in ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Apr. 2024, pp. 11661–11665. doi: 10.1109/ICASSP48485.2024.10448015.

[10] E. Ukwandu et al., “A Review of Cyber-Ranges and Testbeds: Current and Future Trends,” Sensors, vol. 20, no. 24, p. 7148, Dec. 2020, doi: 10.3390/s20247148.

[11] S. M. Khalil, H. Bahsi, H. O. Dola, T. Korõtko, K. McLaughlin, and V. Kotkas, “Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System,” Comput Secur, vol. 124, p. 102950, Jan. 2023, doi: 10.1016/j.cose.2022.102950.

[12] L. Yue and T. Chen, “AI Large Model and 6G Network,” in 2023 IEEE Globecom Workshops (GC Wkshps), IEEE, Dec. 2023, pp. 2049–2054. doi: 10.1109/GCWkshps58843.2023.1046521.