RESEARCH ARTICLE OPEN ACCESS

Ousia : Centralized AI-Driven Vulnerability Detection and Intelligent Query Interface

Prof. Balaji Chaugule, Vivek Tyagi, Yuvraj Patil, Aaryan Nagrale, Aditya Kumbhar
Department of Information Technology
Zeal college of Engineering and research,
Savitribai Phule Pune University
Pune,India

ABSTRACT

Today, security analysts use several tools to assess and evaluate vulnerabilities and threats in order to protect against them. The outputs produced by these tools, however, are often disjointed, and much effort is needed to correlate, analyze, and make decisions. This paper introduces Ousia : an automated Vulnerability Aggregation and Analysis solution, called Centralized AI-Driven Vulnerability Detection and Intelligent Query Interface, which integrates several security scanning tools into a single platform to provide automated vulnerability aggregation and analysis. The proposed system gathers the scan result from various security tools, normalizes security data, correlates the vulnerabilities with threat intelligence sources, and produces detailed security reports with important results. Also, a Retrieval-Augmented Generation (RAG) system is embedded, which uses Large Language Models (LLMs) to deliver contextually appropriate cybersecurity guidance and respond to analyst queries in natural language. The goal of the proposed framework is to decrease the amount of analysis time, enhance situational awareness, and help security practitioners make quicker and more informed decisions. It was experimentally tested on 2,189 cybersecurity assessment queries and the results showed an overall accuracy of 74.97%, validating the proposed intelligent query interface for cybersecurity support.

Keywords:—cybersecurity, Vulnerability Detection, Threat Intelligence, Large Language Models, Retrieval-Augmented Generation, Security Scanning Tools, Intelligent Query Interface, Artificial Intelligence.

I. INTRODUCTION

The cybersecurity field is ongoing through a change where there is increase in attack and use of AI in that attack are significant. Organizations presently rely on penetration testing tools to identify the weakness in their network, applications or system. Various tools such as Nmap, httpx, Katana and many more generate their own security reports related to vulnerability. Operations of all these tools are independent which produces fragmented output that the security analyst to go through process to identify key vulnerability and threat prioritization which is highly complex and time-consuming process.

Vulnerability management systems which are available presently primarily focused on the vulnerability detection rather than the contextual understanding. Hence security teams manually identify key issues through a process which takes a lot of time to identify possible exploitation as wells as correlate the common Vulnerabilities and Exposures (CVE). On other side volume of cybersecurity threat intelligence are also increasing on a rapid pace such as nvd and exploit db. This created an additional challenge for extracting the efficient insights for the security analysts. Automation is the key for this which will significantly improve the capabilities for the cybersecurity analysis process.

Automation through usage of Artificial Intelligence (AI), Large Language Models (LLMs), and Retrieval-Augmented Generation (RAG) would assist analyst onto this process.AI driven approaches help process large volume of vulnerability data and can also provide contextual explanation for detected threats. By integrating RAG-based architectures with cybersecurity datasets, intelligent systems can retrieve relevant threat information in real time and generate accurate, context-aware responses for security analysts through natural language interaction.

Ousia proposes a centralized AI-driven vulnerability detection and intelligent query interface designed to simplify and automate cybersecurity analysis. In this system the user will get unified web-based platform where the user can perform active as well as passive scanning. Fragmented outputs generated through the scans would be normalized into a structured reports containing CVE identifiers, CVSS severity scores, affected services, and vulnerability descriptions. Also, there would be a context-aware RAG-powered chatbot to support natural language queries related to vulnerabilities, exploit techniques, remediation guidance, and cybersecurity threat analysis.

The key contribution of this research is the development of cybersecurity integrated framework including multi-tool vulnerability scanning, threat intelligence correlation and attack path analysis, and AI-powered cybersecurity interaction on one platform. Unlike conventional vulnerability assessment systems, which are mainly oriented towards the detection of vulnerabilities, the proposed solution is based on the understanding of the context

and intelligent

interpretation of vulnerabilities through RAG-enhanced language models. The goal of the system is to minimize manual analysis workload, prioritize vulnerabilities better, and help security analysts to make faster decisions.

II. RELATED WORK

A. *Vulnerability Detection and Management Systems*

Vulnerability assessment tools are widely used to identify security weaknesses in networks, web applications, and information systems. Nmap, Amass, Subfinder, Httpx, Katana, FFUF, SQLMap, Dalfox, Xray, and WafW00f are commonly used tools for identifying security weaknesses in networks, web applications, and digital infrastructures. These tools perform specialized tasks such as network reconnaissance, subdomain enumeration, web crawling, vulnerability scanning, and security testing. They provide valuable security insights; however, the information generated by each tool is typically produced independently and presented in different formats. Consequently, security analysts are required to manually review and correlate findings from multiple tools to identify critical vulnerabilities and prioritize remediation efforts. This fragmented approach increases both the complexity of analysis and the operational workload associated with vulnerability management.

A number of researchers have suggested vulnerability management frameworks to simplify the security assessment process and to enhance risk prioritization. These are designed to combine information from several security products and offer a unified understanding of the security status of an organization. But most of the current solutions are mainly about vulnerability collection and reporting with limited support for contextual interpretation and intelligent analysis. With the number of vulnerabilities continually growing, security analysts need tools that not only identify vulnerabilities, but also help them to understand how they might affect their systems and which vulnerabilities should be addressed first.

B. *Threat Intelligence and Security Information Correlation*

Threat intelligence sources provide valuable information regarding vulnerability severity, exploit availability, attack techniques, and remediation recommendations. Platforms such as the National Vulnerability Database (NVD), ExploitDB, and Shodan are widely used by security professionals to obtain contextual information about detected vulnerabilities. These resources assist analysts in understanding the real-world impact of security weaknesses and identifying actively exploited vulnerabilities. However, existing vulnerability assessment workflows often require manual correlation between vulnerability scan results and threat intelligence repositories. The absence of a centralized mechanism for integrating vulnerability assessment data with threat intelligence information reduces the efficiency of cybersecurity analysis and decision-making processes.

The recent studies have stressed the need to incorporate threat intelligence into the vulnerability management processes. Combining vulnerability data with external intelligence sources can provide greater visibility into the trends of exploits, attacker behavior, and new threats. Threat intelligence enrichment allows analysts to find the most dangerous vulnerabilities currently being exploited by threat actors in the wild, and prioritize remediation accordingly. However, the integration process is still semi-automated, with a significant amount of manual effort, thus highlighting the need for more intelligent and automated threat correlation mechanisms

C. *Artificial Intelligence and Retrieval-Augmented Generation in Cybersecurity*

Recent advancements in Artificial Intelligence (AI), Large Language Models (LLMs), and Retrieval-Augmented Generation (RAG) have created new opportunities for cybersecurity automation and intelligent assistance. AI-powered systems can analyze large volumes of vulnerability data, generate contextual explanations, and assist security analysts in understanding complex security findings. Large Language Models have demonstrated effectiveness in cybersecurity applications such as vulnerability explanation, threat analysis, security report summarization, and question-answering systems.

RAG-based architectures improve the reliability of LLM-generated responses by retrieving relevant cybersecurity knowledge before response generation. Despite these advancements, most existing solutions focus on individual aspects of cybersecurity analysis and do not provide a unified platform that integrates multi-tool vulnerability assessment, threat intelligence correlation, automated report generation, and AI-powered conversational assistance. The proposed research addresses this limitation through the development of a centralized AI-driven vulnerability detection and intelligent query interface that combines these capabilities within a single framework.

III. PROPOSED METHODOLOGY

A. *System Overview*

The proposed system is a single, centralized AI-based framework for Vulnerability Detection & Intelligent Querying that will enable simplified Cybersecurity Analysis & Automated Vulnerability Assessments. The proposed Framework combines numerous vulnerability Scanning Tools and Reconnaissance tools in one Single Platform capable of providing Real-Time Security Analysis results on Target

Domains and Network Hosts. The main goal of this System is to collect all relevant vulnerability information from various Security Tool(s), Normalize Scan Results into Structured Reports, correlate each identified Vulnerability to Threat Intelligence Sources and Provide Cybersecurity Assistance via RAG (Retrieval Augmented Generation) based Chatbot Interface.

.

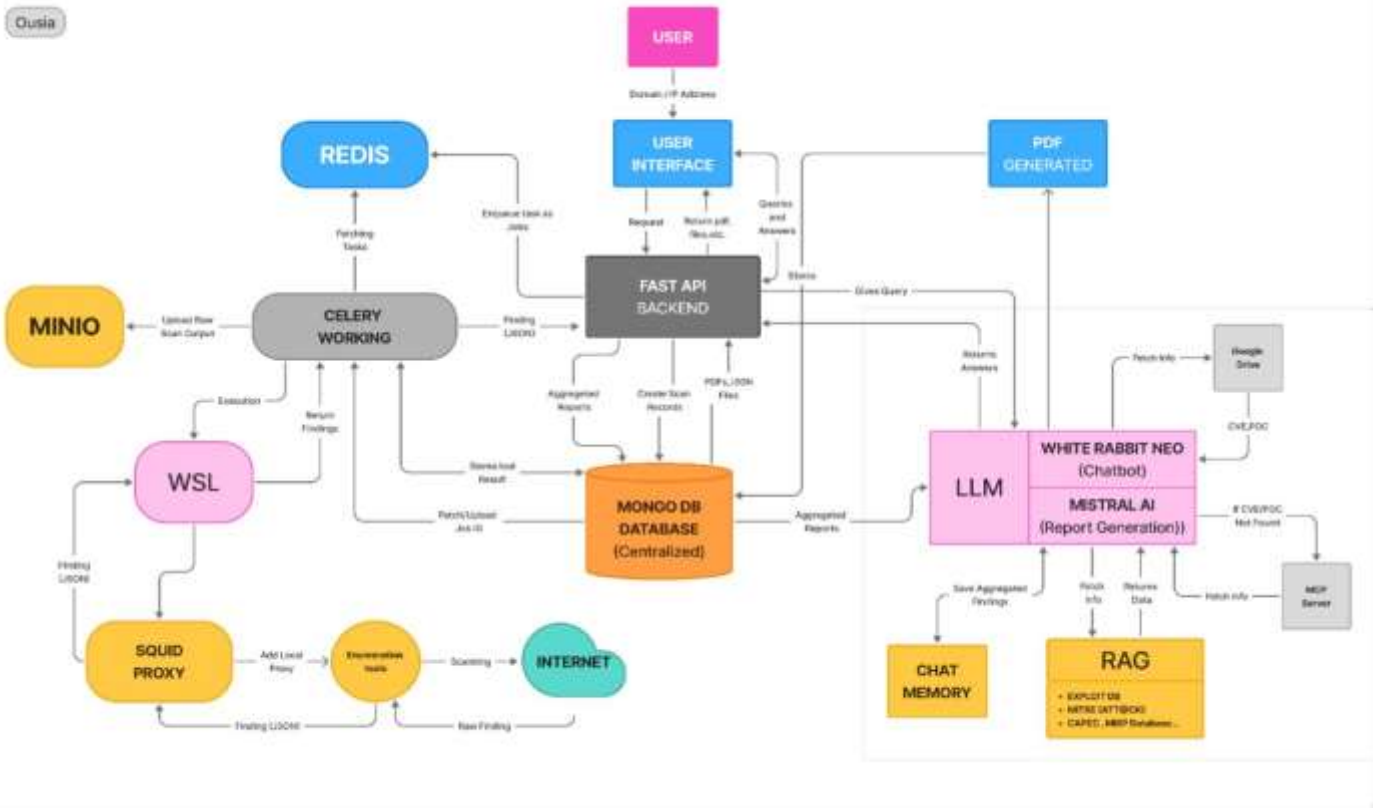

Fig 3.1 System Architecture of the Centralized AI-Driven Vulnerability Detection and Intelligent Query Interface

Vulnerability Scans via the Web Interface; while the Back-End manages the Execution of Tasks, Process the Scans, Aggregate Identified Vulnerabilities & Generate Automated Reports. The Framework was Designed to Support Scalable Asynchronous Task Processing Utilizing Task Queue Management and Centralized Storage Mechanisms.

The vulnerability scanning layer uses various tools in order to perform active and passive network scans on your target systems. All of the generated data from these scans is then converted into structured output (JSON) that is entered into a central database. In addition to providing, you with an analysis of vulnerabilities identified through the use of the previously mentioned tools, the framework also provides you with the ability to correlate the results of those analyses with external sources of information

The Proposed Framework consists of several Interconnected Modules including Web-Based Graphical User Interface, Backend Processing Engine, Layered Vulnerability Scanning, Centralized Database, Data Normalization Module, Threat Intelligence Correlation Engine and AI-Powered Intelligent Query Interface. The System Architecture allows Users to Initiate Active & Passive

such as the national vulnerability database, exploit database, MITRE ATT&CK, CAPEC, and in order to add additional context or references regarding remediations.

B. Vulnerability Assessment and Data Processing Layer

The Vulnerability Assessment and Data Processing Layer will carry out active and passive reconnaissance, asset discovery, technology fingerprinting and vulnerability identification on target systems. The results created are gathered in structured JSON format and fed into the data aggregation and normalization engine. The framework organizes the information collected into a consistent structure with vulnerability identifiers, severity levels, assets impacted, vulnerability descriptions and remediation recommendations. Duplicate findings are deduplicated and correlated to get a single view of security posture.

Table 3.1: Security Assessment and Reconnaissance Tools Integrated within the Proposed Framework

C. Threat Intelligence Correlation Layer

The Threat Intelligence Correlation Layer enriches identified vulnerabilities using external cybersecurity intelligence sources. The framework pulls information from the National Vulnerability Database (NVD), Exploit DB, MITRE ATT&CK, CAPEC, and other threat intelligence repositories to gain more insight on whether there is an exploit available, attack techniques, severity ratings, and mitigation strategies. The system uses vulnerability data to correlate with threat intelligence data to gain deeper context of the vulnerabilities identified. This process helps security analysts to rank vulnerabilities by their potential and ease of exploitation, and aids in decision making and remediation planning.

D.RAG-Based Intelligent Query and Report Generation Layer

The RAG-Based Intelligent Query and Report Generation Layer is the intelligence layer of the proposed framework. All these vulnerabilities, threat intelligence records, exploit references, and remediation information are transformed into vector embeddings and then stored in the Pinecone vector database. The Retrieval-Augmented Generation (RAG) pipeline is used to retrieve relevant information from the user's query, which is then provided to the Mistral AI Large Language Model for generating responses.

The chatbot uses conversational memory to keep track of the context and deliver precise cybersecurity support in a natural language manner. Also, the framework automatically creates structured PDF and JSON reports with details on the vulnerabilities, CVE details, severity, assets impacted, threat intelligence references, and remediation suggestions. This holistic solution allows for seamless vulnerability analysis, intelligent cybersecurity support, and automated reporting all in one place.

IV. EXPERIMENTAL SETUP AND EVALUATION

A. Experimental Environment

The proposed solution involved a web-based architecture with several integrated components, implementing a Centralized AI-Driven Vulnerability Detection and Intelligent Query Interface. To handle user requests, vulnerability assessment workflows, report generation and communication with the intelligent query interface, Fast API was used as the backend framework. To ensure the asynchronous execution of tasks and job scheduling for large-scale vulnerability assessment, Redis and Celery were used. MongoDB was used as the central database to store vulnerability findings, scan reports and threat intelligence information.

Category	Tools
Subdomain Enumeration	Amass, Subfinder, Theharvester
Network Scanning	Nmap
Web Technology Fingerprinting	Wappalyzer, WhatWeb
Web Reconnaissance	Httpx, Katana
Directory and Content Discovery	FFUF
Vulnerability Scanning	Nuclei, Xray
SQL Injection Testing	SQLMap
XSS Detection	Dalfox
WAF Detection	WafW00f
DNS Enumeration	Dig
WHOIS Information Gathering	Whois
OSINT and Intelligence Gathering	Shodan
Automated Reconnaissance Framework	Arjun

Table 4.1: Experimental Configuration of the Proposed Framework

Component	Technology Used
Backend Framework	FastAPI
Database	MongoDB
Task Queue	Celery
Cache/Message Broker	Redis
Vector Database	Pinecone
Large Language Model	WhiterabbitNeo, Mistral AI
Vulnerability Assessment Tools	Amass, Nmap, SQLMap, Dalfox, Xray, etc.
Threat Intelligence Sources	NVD, ExploitDB, MITRE ATT&CK, CAPEC
Output Formats	PDF, JSON

The vulnerability assessment layer included several security tools such as Amass, Subfinder, TheHarvester, Whois, Dig, Nmap, Httpx, Katana, FFUF, SQLMap, Dalfox, Xray, WafW00f, Arjun, Wappalyzer, WhatWeb and Shodan. The backbone of the framework was Pinecone, the vector database, and Mistral AI with WhiteRabbitNeo, the Large Language Model, for intelligent query processing. The design of the overall architecture was determined to enable scalable vulnerability analysis, threat intelligence correlation and AI-driven cybersecurity decision making.

B. Dataset and Evaluation Process

The proposed framework was then tested against a dataset of 2,189 questions that were used in the cybersecurity assessment of the domains. The data set encompassed several cybersecurity areas such as System Security, Application Security, Web Security, Network Security, Penetration Testing, Vulnerability Assessment and Cryptography. The categories were chosen to assess the intelligent query interface's performance on a wide variety of cybersecurity topics. In the evaluation process, users' queries were first embedded into vectors and then compared to the knowledge that the cybersecurity domain has in the vector database. The Retrieval-Augmented Generation (RAG) pipeline was used to extract the most relevant contextual data and pass it to the Mistral AI model for generating responses. The responses generated were then compared with the expected answers to evaluate the effectiveness of the proposed framework in giving accurate cyber security assistance.

C. Evaluation Metrics

The effectiveness of the proposed framework was evaluated with the accuracy as the main criterion of evaluation. The accuracy was determined by the number of correct answers given to the number of

Categories (Count & % of Total Mentions)

Domain	Correct Responses
System Security	751 / 1065
Application Security	580 / 808
Web Security	624 / 773
Network Security	165 / 230
Penetration Testing	388 / 475
Vulnerability Assessment	259 / 334
Software Security	173 / 232
Memory Safety	38 / 48
Cryptography	8 / 14
Overall	**1641 / 2189**

questions in the evaluation. Additionally, domain-wise evaluation was carried out to assess the performance of the framework in various domains of cyber security.

The results were then compared with popular existing LLMs and cybersecurity-focused AI solutions to assess the efficacy of the proposed Agentic architecture. This comparative analysis gave insight into the strengths and weaknesses of the framework and its applicability in vulnerability analysis, threat intelligence interpretation and cybersecurity decision.

V. RESULTS

A. Evaluation Setup

In this chapter we test our integrated security assistant based on RAG. The aim was to determine whether this architecture really could simplify the process of vulnerability detection and attack path analysis to be more efficient than the current solutions. We compared our Phase 3 implementation with the industry-leading Large Language Models (LLMs) such as proprietary models like GPT-4-Turbo and GPT-3.5-Turbo and open-source models like Yi-6B, Orca-2-7b and Mistral-7B.

The assessment was done on the ability to interpret raw security reports, describe the threats in the context, and provide actionable remediation suggestions. The evaluation also measured the ability of each model to utilize cybersecurity knowledge effectively across multiple domains includes system security, web security, vulnerability assessment, penetration testing, and cryptography.

B. Dataset Distribution Analysis

Figure 5.1: Distribution of Cybersecurity Questions Across Different Security Domains

The evaluation set comprised cybersecurity questions from various areas such as System Security, Application Security, Web Security, Penetration Testing, Vulnerability Assessment, Software Security, Network Security, Memory Safety and Cryptography. The highest percentage of questions covered System Security (26.8%), followed by Application Security (20.3%) and Web Security (19.4%). This distribution allowed for assessment of the proposed framework across a wide range of cybersecurity topics.

Table 5.1: Domain wise correct responses obtained by Ousia

The domain-wise correct responses obtained by the proposed Ousia framework during evaluation. Out of a total of 2,189 cybersecurity assessment questions, the framework correctly answered 1,641 questions, achieving an overall accuracy of 74.97%. The highest number of correct responses was observed in System Security (751/1065), followed by Web Security (624/773) and Application Security (580/808). Strong performance was also achieved in Penetration Testing (388/475) and Vulnerability Assessment (259/334), demonstrating the effectiveness of the RAG-based architecture in handling practical cybersecurity tasks. These results indicate that Ousia is capable of providing reliable and context-aware cybersecurity assistance across a broad range of security domains.

The distribution of the data mimics real-world cybersecurity scenarios and the fact that security analysts often facechallenges in areas of system configuration, application security and web application security. The introduction of several security domains allowed a thorough evaluation of the framework's relevance to retrieve information, understand the concepts in each domain, and provide context-appropriate answers. This balanced evaluation method will create a framework that is representative of the effectiveness of the framework for a variety of cybersecurity tasks and not just one type of security analysis.

C. Comparative Performance Analysis

Table 5.2: Performance Comparison of the Proposed Framework with Existing Large Language Models

Model	System	App	Web	Network	PenTest	Vuln	Crypto	Overall
GPT-4-Turbo	73.61	75.25	82.15	75.65	80.00	76.05	64.29	79.07
Ousia	70.52	71.78	80.72	71.74	81.68	77.54	57.14	74.97
GPT-3.5-Turbo	59.15	57.18	63.00	60.87	72.00	60.18	35.71	62.09
Yi-6B	50.61	48.89	54.98	36.52	69.26	49.40	35.71	53.57
Orca-2-7b	46.76	47.03	55.63	49.13	60.84	50.00	14.29	51.60
Mistral-7B-v0.1	40.19	38.37	46.57	36.52	53.47	42.22	28.57	43.65
chatglm3-6b	39.72	37.25	41.14	43.04	57.47	37.43	28.57	41.58
Llama-2-7b-hf	20.94	18.69	22.77	14.35	26.11	21.56	21.43	22.15

The comparative performance of the proposed Agentic framework named Ousia is shown in Table 5.1 with some of the proprietary and Open-Source Large Language Models. The results demonstrate that GPT-4-Turbo has the best overall accuracy (79.07%), whereas the proposed Ousia framework achieves an overall accuracy of 74.97%. In the Penetration Testing and Vulnerability Assessment categories, the proposed framework showed higher accuracy of 81.68% and 77.54% respectively than GPT-4-Turbo. These findings confirm the efficacy of using the Retrieval-Augmented Generation and cybersecurity specific knowledge sources in the analysis process.

The performance results also show that the use of external cybersecurity knowledge is a significant boost to the ability of the model to respond to domain-specific cybersecurity questions. Although general-purpose language models make use of pre-trained knowledge, the proposed Ousia framework gains from the retrieval of relevant vulnerability information, threat intelligence records, references to exploits, and remediation guidance when it comes to generating responses. This context-based foundation allows the framework to offer more precise and reliable cybersecurity support, especially in practical areas like vulnerability assessment and penetration testing, where the most recent security information is vital.

VI. CONCLUSION

The increasing complexity of modern cyber threats and the widespread use of multiple security assessment tools have made vulnerability analysis a challenging and time-consuming task for security professionals. Current vulnerability management methods tend to produce disjointed results, which are hard to correlate, prioritize and interpret manually. Moreover, with the ever-increasing amount of threat intelligence information, it's harder to find actionable security insights.

This research proposed an approach for Centralized AI-Driven Vulnerability Detection and Intelligent Query Interface, aimed at making cybersecurity analysis easier and automated. The proposed framework will combine several vulnerability assessment and penetration testing tools in a single platform, allowing for the collection, normalization, and analysis of security findings in a central location. Experimental evaluation on 2,189 cybersecurity assessment questions demonstrated an overall accuracy of 74.97%, validating the effectiveness of Ousia for vulnerability analysis and intelligent cybersecurity assistance. The framework can be integrated with threat intelligence feeds to correlate vulnerabilities with threat information, and it can be used to create structured security reports, which enhances the efficiency of vulnerability management processes.

The system also uses a Large Language Model (LLM) to provide an intelligent assistant that supports contextual understanding and increases the productivity of the analyst by leveraging a Retrieval-Augmented Generation (RAG) approach. The smart query interface allows users to use natural language to interact with cybersecurity information and receive contextual explanations, remediation steps, and threat intelligence information. The effectiveness of the proposed approach for cybersecurity analysis and decision-making was validated in an experimental evaluation.

The proposed framework will help to minimize manual analysis efforts, prioritize vulnerabilities, and support security analysts to make quicker and better security decisions. Future research could involve the development of real-time threat monitoring systems, automated attack path generation, integration with Security Information and Event Management (SIEM) systems, and leveraging advanced Large Language Models for enhanced accuracy and functionality in intelligent cybersecurity support systems.

ACKNOWLEDGMENT

The authors gratefully acknowledge the researchers and academic resources whose contributions supported this study.

REFERENCES

[1] Y. Hu, F. Zou, J. Han, X. Sun, and Y. Wang, “LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model,” Computers & Security, vol. 145, p. 103999, 2024.

[2] Y. Zhou, Y. Tang, M. Yi, C. Xi, and H. Lu, “Security and communication networks,” Wiley Online Library, 2022.

[3] J. Kotsias, A. Ahmad, and R. Scheepers, “Adopting and integrating cyber-threat intelligence in a commercial organisation,” European Journal of Information Systems, vol. 32, no. 1, pp. 35–51, 2023.

[4] D. R. Arikkat et al., “IntellBot: Retrieval augmented LLM chatbot for cyber threat knowledge delivery,” in Proc. 2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN), 2024.E.A. Patil, P. Deore, P. Patil, A. Talekar, and M. Mali, ‘‘ForenSift: Gen-AI powered integrated digital forensics and incident response platform using LangChain framework,’’ Digit. Forensics Secur. Appl., vol. 2024, pp. 1–15, Jul. 2024.

[5] Y. Hmimou, M. Tabaa, A. Khiat, and Z. Hidila, “A multi-agent system for cybersecurity threat

detection and correlation using large language models," IEEE Access, vol. 13, pp. 150199–150220, 2025.

[6] K. Afane, W. Wei, Y. Mao, J. Farooq, and J. Chen, "Next-generation phishing: How LLM agents empower cyber attackers," unpublished.

[7] T. Ze Micheal, J. Yang, and A. Doupe, ''LLM agents for vulnerability identification and CVE verification,'' in Proc. CEUR Workshop, vol. 3562, 2024. [Online]. Available: https://ceur-ws.org/Vol-3562/.

[8] N. Tihanyi, M. A. Ferrag, R. Jain, T. Bisztray, and M. Debbah, "CyberMetric: A benchmark dataset based on retrieval-augmented generation for evaluating LLMs in cybersecurity knowledge," 2024, arXiv:2402.04211. [Online]. Available: https://arxiv.org/abs/2402.04211

[9] "Current CVSS Score Distribution For All Vulnerabilities." CVE Security Vulnerability Database. Security Vulnerabilities, Exploits, References and More. Last accessed April 6th, 2021. https://www.cv edetails.com/cve/CVE-2019-15107/.

[10] Y. E. Seyyar, A. G. Yavuz, and H. M. Ünver, "An attack detection framework based on BERT and deep learning," IEEE Access, vol. 10, pp. 68633–68644, 2022.

[11] V. Rathod, S. Nabavirazavi, S. Zad, and S. S. Iyengar, "Privacy and security challenges in large language models," in Proc. IEEE CCWC 2025, 2025.

[12] C. Rodriguez, S. Zamanirad, R. Nouri, K. Darabal, B. Benatallah, and M. Al-Banna, "Security vulnerability information service with natural language query support," in Proc. CAiSE 2019, 2019.

[13] A. A. Siam, M. Alazab, A. Awajan, and N. Faruqui, "A comprehensive review of AI's current impact and future prospects in cybersecurity," IEEE Access, vol. 13, pp. 14025–14061, 2025.

[14] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: A comprehensive review of AI-driven detection techniques," J. Big Data, vol. 11, no. 1, p. 105, Aug. 2024.

[15] M. A. Ferrag et al., "MCM-Llama: A fine-tuned large language model for real-time threat detection through security event," IEEE Access, vol. 12,pp. 115543–115558, 2024.

[16] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions," Frontiers in Big Data, vol. 7, Art. no. 1497535, 2024.

[17] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," IEEE Access, vol. 10, pp. 93104–93139, 2022.

[18] N. Ilg, M. Pfitzenmaier, D. Germek, P. Duplys, and M. Menth, "ALDExA: Automated LLM-assisted detection of CVE exploitation attempts in host-captured data," IEEE Access, vol. 13, pp. 95379–95391, 2025.

[19] X. Zhou, T. Zhang, and D. Lo, "Large language model for vulnerability detection: Emerging results and future directions," in Proc. 2024 ACM/IEEE 44th International Conference on Software Engineering (ICSE), 2024.

[20] C. Islam, M. A. Babar, R. Croft, and H. Janicke, "SmartValidator: A framework for automatic identification and classification of cyber threat data," unpublished.

[21] K. Dhanushkodi and S. Thejas, "AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation," IEEE Access, vol. 12, pp. 173135–173136, 2024.

[22] S. Sai, U. Yashvardhan, V. Chamola, and B. Sikdar, "Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space," IEEE Access, vol. 12, pp. 43109–43146, 2024.

[23] I. Prieto and B. Blakely, "Proposed uses of generative AI in a cybersecurity-focused soar agent," in Proc. AAAI Symposium Series, 2023.

[24] D. B. Cruz, J. R. Almeida, and J. L. Oliveira, "Open-source solutions for vulnerability assessment: A comparative analysis," IEEE Access, vol. 11,p. 100234–100255, 2023.

[25] P. Lachkov, L. Tawalbeh, and S. Bhatt, ''Vulnerability assessment for applications security through penetration simulation and testing,'' J. Web Eng., vol. 21, pp. 2187–2208, Dec. 2022

[26] W. Kasri, Y. Himeur, H. A. Alkhazaleh, S. Tarapiah, S. Atalla, W. Mansoor and H. Al-Ahmad, ''From vulnerability to defense: The role oflarge language models in enhancing cybersecurity,'' Computation, vol. 13, no. 2, p. 30, Jan. 2025, doi: 10.3390/computation13020030

[27] M. Mudassar Yamin, E. Hashmi, M. Ullah, and B. Katt, ''Applica-tions of LLMs for generating cyber security exercise scenarios,'' IEEE

Access, vol. 12, pp. 143806–143822, 2024, doi: 10.1109/ACCESS.s2024.3468914.

.

[28] E. Pleshakova, A. Osipov, S. Gataullin, T. Gataullin, and A. Vasilakos,‘‘Next gen cybersecurity paradigm towards artificial general intelligence:Russian market challenges and future global technological trends,’’ J.Comput. Virol. Hacking Techn., vol. 20, no. 3, pp. 429–440, Jul. 2024, doi:10.1007/s11416-024-00529-x.

[29] Blakely, B. 2022.An Experimental Platform for Au-tonomous Intelligent Cyber-Defense Agents: Towards a col-laborative community approach (WIPP). InResilience Week2022. National Harbor, Maryland, USA: IEEE