International Journal of Engineering Trends and Applications (IJETA) – Volume 13 Issue 3, May-Jun 2026

RESEARCH ARTICLE OPEN ACCESS

AI-Driven Vulnerability Detection: A Survey and Motivation for Centralized Conversational Security Systems

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

ABSTRACT

In modern world the cybersecurity field rely on multiple platform and tool for performing their operations. In present systems generation of scan reports are fragmented where analysts need to manually analyze the report and tell about the security risks. This paper proposes a centralized vulnerability detection and intelligent query interface that integrates multiple security scanning tools into a unified platform and based on all scan results it generates a report identifying key issues furthermore also providing rag based intelligent assistant which will help understanding and answer any related queries to it. Purpose of this solution is to provide assist to security analysts for faster decision making through AI-powered contextual cybersecurity assistance.

Keywords:—***cybersecurity, large language models, vulnerability detection, threat intelligence, AI systems, centralized security, automated analysis***

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.

Our idea proposes 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. Summary of Current Approaches

Contemporary threat intelligence and vulnerability analysis approaches exhibit significant diversity in methodological approaches, data sources, and analytical frameworks. Traditional approaches rely heavily on signature-based detection systems, vulnerability databases such as the National Vulnerability Database (NVD), and expert-curated threat intelligence feeds that provide indicators of compromise and attack attribution information.

The emergence of machine learning approaches has introduced data-driven threat analysis capabilities that complement traditional rule-based systems. Recent research

demonstrates the application of large language models to threat intelligence knowledge graph construction, enabling automated extraction of threat entities, relationships, and tactics from unstructured sources [1]. Approaches such as LLM-TIKG leverage few-shot learning capabilities to reduce manual annotation requirements while improving the semantic modeling of complex threat relationships [20].

Multi-agent architectures represent another significant advancement in threat analysis capabilities [6]. Various studies represent that a modular multi-agent system that integrates established cybersecurity tools with large language models to achieve threat detection accuracy and multi-agent correlation accuracy while reducing false positives. Their approach demonstrates the effectiveness of combining domain-specific tools with semantic analysis capabilities to detect complex threat patterns that evade isolated detection mechanisms. Also, integration of retrieval-augmented generation (RAG) architectures has emerged as a particularly promising approach for threat intelligence processing. RAG based system combines that LLMs with RAG models delivers superior threat intelligence capabilities [4].

Approaches stresses on the importance that focus on contextual threat correlation. The existing vulnerability scanners can only catch individual weaknesses rather than illustrate their interrelations, and thus limit the utility of them for cyber defenders. Weaknesses are frequently leveraged in combination with coordinated attacks or associated to threat campaigns. Studies addresses the issue and also started to discuss about the weakness in approach. Enhancement with knowledge graph-based and context-aware method are initiated.

B. Role of AL and LLM in cybersecurity automation

Large language models have emerged as a stalemate changing technology in the domain of cybersecurity. Applicability of LLM in the cybersecurity automation technology, which offers an unmatched natural language processing, human-machine interface, context, and human-machine interface. The LLMs do cross disciplines in the cybersecurity domain. Some of the fields where the application of LLM is evident include response generation, vulnerability analysis, malware recognition and threat intelligence processing.

Recent research describes comprehensive analysis of LLM applications in cybersecurity, examining both defensive applications such as threat detection [16] and analysis, as well as potential misuse scenarios where LLMs assist in attack generation and evasion [7]. Their survey reveals that while LLMs demonstrate significant promise in enhancing cybersecurity capabilities, concerns about adversarial robustness and model interpretability remain persistent challenges that limit widespread adoption in security-critical applications.

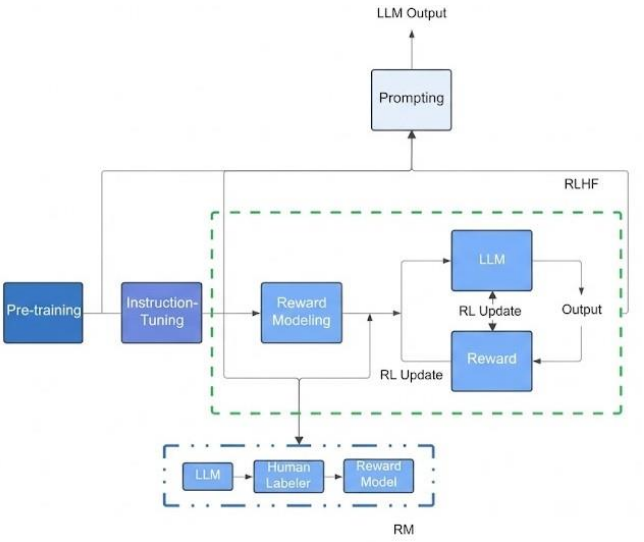

Fig. 1. Overview of LLM Workflow

The standard training architecture of Large Language Models (LLM), upon which current cybersecurity automation is based. The first stage is the Pre-training on huge amounts of data to gain linguistic skills, and the second stage is Instruction-Tuning to tailor the model to particular task-related behaviors. An important constituent displayed is Reinforcement Learning through Human Feedback (RLHF) in which the output produced by the LLM is directed by a Reward Model (RM), which is trained by human labelers, to produce not only accurate outputs but also safe and useful outputs. Applied to cybersecurity, this pipeline enables to be specialized to specific purposes including automated vulnerability detection, threat intelligence generation, and real-time incident response, where human-consistent reasoning is needed to operate within complex, adversarial settings.

Another area of application of LLMs in cybersecurity automation is conversational security systems. Recent studies examine how retrieval-augmented generation (RAG) can be combined with large language models to support contextual reasoning on external sources of security knowledge. Conversational interfaces, like IntellBot, show how threat intelligence exploration, analyst queries, and knowledge delivery can be supported by combining LLM reasoning with both structured and unstructured threat data [4].

C. Observational Insights

The review of current literature demonstrates that Retrieval-Augmented Generation (RAG) has emerged as the best practice for providing context-aware security advice and also outperforms pure fine-tuning which have hallucination problem. However, the disaggregation of cybersecurity tools poses a tremendous challenge to the overall threat analysis and response. It is critical for specific organization's network topology or existing defenses. The existing systems have minimal support of natural language interaction and query in context.

Research shift in agent related to cybersecurity from just a simple question-answer chatbot like IntellBot [4] towards the

reasoning agents [9]. Future of agents would not only be only to detect a threat but also provide response to it whose implementations have already begun [24]. Frameworks proposed by Hmimou et al. (2025), also reflects agent use where specialized agents for different purpose which operates independently.

III. AI TECHNIQUES FOR VULNERABILITY DETECTION

Artificial intelligence techniques have significantly enhanced vulnerability detection by enabling automated analysis of large-scale and complex security data. Traditional machine learning approaches such as Support Vector Machines, Decision Trees, and Random Forest have been widely used for identifying patterns in vulnerable code and network traffic. These methods rely on feature engineering and are effective in structured environments but often struggle with unstructured data and evolving attack patterns [11], [22].

Deep learning techniques, including Convolutional Neural Networks and transformer-based models such as BERT, have improved detection capabilities by enabling automatic feature extraction and contextual analysis. For instance, BERT-based frameworks have demonstrated effectiveness in identifying attack patterns and anomalies in cybersecurity datasets [11]. These approaches reduce manual effort but require large datasets and computational resources.

More recently, Large Language Models (LLMs) have emerged as a powerful tool for vulnerability detection and threat intelligence analysis. Systems such as LLM-TIKG [1] and MCM-Llama [16] leverage LLMs to construct knowledge graphs, correlate security events, and enhance contextual understanding of vulnerabilities. Additionally, retrieval-augmented approaches, such as IntellBot [4], integrate external knowledge sources to improve response accuracy and reduce hallucination. LLM-based systems also enable automated reasoning, natural language interaction, and real-time threat analysis [20].

Furthermore, multi-agent systems and LLM-assisted frameworks have been proposed to improve coordination and decision-making in cybersecurity environments. These systems allow distributed agents to collaborate and process threat intelligence more effectively [6], [19]. However, challenges such as explainability, privacy concerns, and generalization across diverse environments remain significant limitations [12], [18].
Overall, the integration of machine learning, deep learning, and LLM-based techniques provides a comprehensive approach to vulnerability detection, combining pattern recognition, contextual understanding, and intelligent automation.

IV. COMPARATIVE ANALYSIS

A. Source Selection and Paper Evaluation Method

The systematic literature analysis methodology is selected in this study because research articles published in recent times analyzed, evaluated, and discussed in order to learn about the application of artificial intelligence and large language models to cybersecurity by attackers as well as defenders. The process of selection focuses on the approach of rigor in methods, their empirical validation, and their relevance to the fundamental cybersecurity actions, vulnerability detection, threat intelligence processing, security automation, and support of the analogy. The literature review practice is conducted in accordance with the screening principles of PRISMA, which allows making consistent inclusion and exclusion decisions in large academic repositories such as IEEE Xplore, ACM Digital Library, ScienceDirect, and other archival sources. It is a protocol that helps use quality studies since it filters peer-reviewed articles, verified experimental designs, and concise evaluation strategies. In the selected literature, it can be noted that extensively the works are reflective-defensive and dual-use AI applications in software, network, cloud, and infrastructure security.

A change in the evaluation approach used in the reviewed studies can be seen as the transition of the single, statistical anomaly detection techniques to multi-layered evaluation frameworks. These models combine qualitative synthesis and quantitative benchmarking, often controlled experimental testbeds and field data. Examples of common evaluation metrics are precision, recall, F1-score, Cohen Kappa, and AUC, and some of the studies additionally use meta-analysis and risk-of-bias (RoB) assessments to determine the robustness of the results. The multi-agent assessment pipelines and the addition of the repository-level and Just-in-Time (JIT) vulnerability detection benchmarks are used to ensure that both the operational realism and the depth of analysis are covered by the reviewed studies.

B. Thematic Classification of the Reviewed Studies

As it can be perceived in accordance with the functional goals and the characteristics of the architecture as reflected in the selected literature, the reviewed works can be divided into four large classes that reflect the situation in the modern landscape of AI- and LLM-based study of cybersecurity issues. AI-Based Vulnerability Detection and Program Analysis in which this branch is the focus of research seeking to detect the vulnerabilities in the software, categorize and remediate the vulnerabilities with the aid of machine learning, deep learning, and reasoning using the aid of LLM. Other studies under this category concern function level, repository level and Just in Time vulnerability detection, and automated program repair. Representative systems focus on contextual reasoning among interprocedurally code paths and pairwise comparisons of vulnerable and patched commits. These techniques are extraction, organization, and inference of heterogeneous sources of cyber threat intelligence with the purpose of providing intelligence. The literature seeks to mention the LLM based named entity recognition, tactic and technique extraction and semantic alignment between structured taxonomies (e.g., CVE, CWE) and non-structured threat reports. The graph construction of knowledge and the pipelines of the CTI reasoning is an important aspect in this category.

Those that utilize LLMs in automating the work of analysts, natural-language querying, retrieval-augmented generation, and decision support belong to the LLM-Enabled Automation

and Conversational Security Systems group. The studies reviewed show the potential of conversational interfaces and RAG architectures to decrease the workload of analysts, speed up investigations, and enhance access to the complex security data. Multi- Agent and Centralized Security Architectures. The category of research in this area looks into distributed and agent-based models that are meant to combine several security activities into a single reasoning and orchestration layer. The multi-agent systems that utilize reasoning-action-observation cycles are meant to scale and should be automated so as to remediate and provide coordinated analysis across varied data sets and security tools.

C. Analytical Framework for synthesizing Insights

The section is a synthesis of technical qualities and performance features, which were obtained after the evaluation of all studies reviewed. The comparative analysis indicates a clear transition from traditional rule-based approaches to advanced AI-driven methods in vulnerability detection. Machine learning techniques enhance classification accuracy by utilizing structured data, whereas deep learning models enable automatic feature extraction from complex inputs such as source code and network traffic. Furthermore, large language model-based systems demonstrate improved contextual understanding, particularly in processing unstructured threat intelligence. However, the effectiveness of these approaches is significantly influenced by dataset quality, model architecture, and their ability to generalize across different operational environments. This highlights the need for more standardized evaluation frameworks and robust validation techniques in future research.

TABLE I. COMPARISON OF LLM BASED CYBER FRAMEWORKS

Paper	Technique	Dataset	Performance	Limitation
[1] LLM-TIKG (2024)	LLM + Few-shot Learning	Not Reported	87.88% precision (entity recognition)	Limited generalization across domains
[4] IntellBot (2024)	RAG + LLM	Not Reported.	High similarity scores (0.8–1.0)	Performance depends on data quality
[6] Multi-Agent System (2025)	Multi-agent + LLM	Not Reported	93.6% detection accuracy	Complex system design
[9] Systematic Review (2025)	Literature Review	Multiple sources	Identified emerging trends	Complex system design
CyberMetric (2024)	Benchmark Dataset + LLM	Custom dataset (10,000 Q&A)	High performance of LLMs	Limited real-world testing
MCM-Llama (2024)	Fine-tuned LLM	CTU-13 dataset	Improved alert correlation	Dataset Dependency
Generative AI Survey (2024)	Generative AI Analysis	Not Reported	Conceptual insights	Lack of quantitative evaluation

V. CHALLENGES AND RESEARCH GAPS

A. Fragmentation of Cybersecurity Tools and Data Sources

The contemporary cybersecurity landscape exhibits significant fragmentation across tools, data formats, and analytical frameworks that impedes comprehensive threat analysis and coordinated response efforts. Organizations typically deploy multiple point solutions for different security functions including vulnerability scanning, threat intelligence, intrusion detection, and incident response, each operating with distinct data models and interfaces.

This fragmentation creates several critical challenges for effective security operations. First, data correlation across disparate systems require manual effort and introduce delays in threat identification and response. Security analysts must synthesize information from multiple dashboards and reports, increasing cognitive load and creating opportunities for oversight of complex attack patterns that span multiple security domains.

B. Lack of Real-Time Intelligent Vulnerability Correlation

Traditional vulnerability management approaches operate on scheduled scanning cycles that may miss rapidly evolving threats and fail to provide real-time awareness of changing risk profiles. Most vulnerability scanners execute daily or weekly scans that generate static reports requiring manual analysis to understand threat implications and prioritize remediation efforts.

This temporal limitation becomes particularly problematic in dynamic environments where new vulnerabilities emerge rapidly and threat actors adapt their techniques to exploit recently disclosed weaknesses. The lag between vulnerability disclosure and organizational awareness creates windows of opportunity that sophisticated attackers routinely exploit. Existing cybersecurity systems demonstrate significant limitations in contextual analysis and reasoning capabilities that prevent comprehensive understanding of threat implications and attack narratives. Traditional rule-based systems operate on predefined patterns that cannot adapt to novel attack techniques or understand the strategic context of observed activities.

Current vulnerability assessment tools identify individual weaknesses but fail to analyse how these vulnerabilities might be chained together in multi-stage attacks or exploited in conjunction with social engineering techniques. This limitation prevents organizations from understanding realistic.

Despite the advancements in AI-driven vulnerability detection, several critical challenges remain. Many existing approaches rely heavily on benchmark datasets, which may not accurately represent real-world and evolving cyber threats. Additionally, models trained on specific datasets often face difficulties in generalizing across different environments and programming languages. Another significant concern is the lack of explainability in complex models such as deep learning and large language models, which limits trust in security-critical applications. Furthermore, the majority of systems are not evaluated against adversarial scenarios, raising concerns about their robustness. These limitations highlight the need for more reliable, transparent, and scalable solutions in future research

VI. FUTURE RESEARCH DIRECTIONS

A. Emerging AI Trends for Autonomous Vulnerability Detection

The evolution toward autonomous vulnerability detection represents a significant frontier in cybersecurity research, with implications for fundamentally changing how organizations approach threat management. Current research trends indicate movement toward self-healing security systems that can automatically identify, analyse, and remediate vulnerabilities without human intervention, though significant challenges remain in achieving the reliability and trustworthiness required for fully autonomous operation.

Federated learning approaches show promise for enabling collaborative threat detection while preserving organizational privacy. These approaches allow multiple organizations to contribute to vulnerability detection model training without sharing sensitive data, potentially creating more robust detection capabilities than any single organization could develop independently.

B. LLM Integration with Real-Time Threat Feeds

The integration of large language models with real-time threat intelligence feeds presents significant opportunities for enhancing situational awareness and predictive threat analysis. Current research explores techniques for processing streaming threat data through transformer architectures to identify emerging patterns and predict future attack trends with greater accuracy than traditional approaches.

Real-time natural language processing of threat intelligence sources including security advisories, research publications, social media discussions, and dark web communications could provide early warning capabilities for emerging threats. However, research challenges include managing the computational requirements for real-time LLM processing while maintaining analytical accuracy.

C. Explainable AI for Secure Decision-Making

The development of explainable AI techniques specifically adapted for cybersecurity contexts represents a critical research area for building trust and enabling validation of automated security decisions. The existing explainability methods created in the context of general machine learning do not necessarily meet the specific needs of the cybersecurity setting and its limitations. Detection logic needs to provide security-specific techniques of explanation that meet various stakeholder needs such as the require detail of the technical analysts, strategic assessment of risk to the management and auditors who need documentation of compliance.

D. Proposed centralized AI-Driven Framework

Based on the analysis presented in this study, a promising direction for future research is the development of a centralized vulnerability detection framework that integrates large language models with real-time threat intelligence and multi-agent coordination. Such a system can effectively reduce tool fragmentation and enable unified analysis across multiple data sources. By combining contextual understanding with automated reasoning, this approach has the potential to improve detection accuracy and response efficiency. Additionally, incorporating explainable AI techniques can enhance trust and usability in security-critical environments.

VI.CONCLUSION

This study highlights key challenges in current cybersecurity systems, including tool fragmentation, lack of intelligent correlation, and limited contextual reasoning capabilities. Existing approaches often operate in isolation, resulting in inefficient threat analysis and delayed response mechanisms. The survey demonstrates that artificial intelligence, particularly large language models, has significantly improved vulnerability detection and threat intelligence processing. These techniques provide enhanced contextual understanding, reduce false positives, and support more efficient security operations compared to traditional methods. Based on the analysis, the development of centralized and intelligent security systems is essential for addressing the limitations of existing approaches. Integrating automated analysis, real-time data correlation, and conversational interfaces can enable more effective and scalable solutions.

Overall, this work emphasizes the growing importance of AI-driven approaches and highlights their potential to transform cybersecurity through improved automation, contextual reasoning, and unified threat management.

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.

[5] E. Adamopoulou and L. Moussiades, "An overview of chatbot technology," in IFIP International Conference on Artificial Intelligence Applications and Innovations, Springer, 2020.

[6] 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.

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

[8] S. Zhang et al., "When cyber meets LLM: A systematic literature review," Cybersecurity, vol. 8, no. 1, pp. 1–41, 2025.

[9] 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

[10] "Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT IIoT devices," unpublished.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] 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.

[23] 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.

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

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