

# LLM-Assisted Proactive Threat Intelligence for Automated Reasoning

Shuva Paul, *Member, IEEE*, Farhad Alemi, *Student Member, IEEE*, and Richard Macwan, *Member, IEEE*

**Abstract**—Successful defense against dynamically evolving cyber threats requires advanced and sophisticated techniques. This research presents a novel approach to enhance real-time cybersecurity threat detection and response by integrating large language models (LLMs) and Retrieval-Augmented Generation (RAG) systems with continuous threat intelligence feeds. Leveraging recent advancements in LLMs, specifically GPT-4o, and the innovative application of RAG techniques, our approach addresses the limitations of traditional static threat analysis by incorporating dynamic, real-time data sources. We leveraged RAG to get the latest information in real-time for threat intelligence, which is not possible in the existing GPT-4o model. We employ the Patrwl framework to automate the retrieval of diverse cybersecurity threat intelligence feeds, including Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Exploit Prediction Scoring System (EPSS), and Known Exploited Vulnerabilities (KEV) databases, and integrate these with the `a11-mpnet-base-v2` model for high-dimensional vector embeddings, stored and queried in Milvus. We demonstrate our system’s efficacy through a series of case studies, revealing significant improvements in addressing recently disclosed vulnerabilities, KEVs, and high-EPSS-score CVEs compared to the baseline GPT-4o. This work not only advances the role of LLMs in cybersecurity but also establishes a robust foundation for the development of automated intelligent cyberthreat information management systems, addressing crucial gaps in current cybersecurity practices.

**Index Terms**—Large Language Models, Cybersecurity, Automated Reasoning, Retrieval Augmented Generation, Threat Intelligence.

## I. INTRODUCTION

### A. Context and Motivation

In the dynamic field of cybersecurity, traditional methods often fail to address the sophisticated and evolving nature of contemporary threats [1]. Incorporating machine learning techniques, particularly large language models (LLMs), into cybersecurity practices presents a promising avenue for enhancing threat detection and response mechanisms. LLMs like BERT [2] and GPT-3 [3] have demonstrated significant advancements in comprehending and generating human-like text, which can be used to process and analyze security-related data. The development of more advanced models, such as GPT-4 [4], extends these capabilities further, offering deeper contextual understanding and more effective generative functions.

The effectiveness of these models is markedly enhanced when combined with Retrieval-Augmented Generation (RAG)

Farhad Alemi is a graduate researcher at Arizona State University. Shuva Paul and Richard Macwan are researchers at the National Renewable Energy Laboratory, Golden, CO

techniques, which merge external information with the generative capabilities of LLMs [5]. We illustrate that, in cybersecurity, RAG systems can be especially beneficial in integrating real-time threat intelligence feeds, providing a more comprehensive and current understanding of the threat landscape.

Despite the advancements in LLMs and RAG systems, there is a notable gap in their application to real-time cybersecurity solutions. Traditional cybersecurity methods often struggle to keep pace with the swiftly evolving nature of cyberthreats [1]. To our knowledge, although LLMs have shown promise in static analyses, their application in dynamic, real-time threat information management remains underexplored. Current RAG systems do not fully integrate continuous threat intelligence feeds, which limits their effectiveness in real-time scenarios [6].

### B. Research Contributions

This research aims to develop and evaluate a novel RAG-based cyber-reasoning system that incorporates continuous threat intelligence feeds for real-time cybersecurity applications. The study seeks to bridge existing gaps in the literature by making the following contributions:

- 1) Integrating continuous threat intelligence with RAG systems: Developing a framework that seamlessly incorporates continuous threat intelligence feeds with RAG systems to enhance real-time threat detection and response capabilities.
- 2) Advancing the use of LLMs in real-time threat analysis: Extending the application of advanced LLMs, such as GPT-4o (“o” for “omni”) [7], for continuous and dynamic threat management.
- 3) Investigating the potential vulnerability of RAG-based systems against adversarial attacks and proposing mitigations.

By addressing these objectives, this research aims to enhance the capabilities of automated cybersecurity systems and pave the way for future innovations in intelligent threat management.

The rest of the manuscript is organized as follows: Section II provides an overview of fundamental concepts relevant to the study. Section III examines current advancements in LLMs and RAG techniques for cybersecurity and identifies research gaps. Section IV describes the experimental setup, data sources, and the proposed RAG-based system framework. Section V presents findings from the experiments conducted to evaluate the proposed system. Section VI summarizes the key findings and highlights the research contributions. Finally, Section VII discusses potential future directions for building upon current findings and advancing the forefront of scientific research.

## II. BACKGROUND

### A. Cybersecurity Metrics:

Cybersecurity standards and frameworks offer structured guidelines to safeguard information systems against cyberthreats. These frameworks enable organizations to systematically identify, manage, and mitigate risks, ensuring robust defense against increasingly sophisticated cyberattacks.

1) *Common Vulnerabilities and Exposures (CVEs)*: The CVE program was initiated by the MITRE Corporation in 1999 [8], [9], [10]. Each vulnerability under this program is assigned a unique identifier by the CVE Numbering Authority (CNA) [11]. As of this writing, there are 255,158 published CVE entries [12].

2) *Common Weakness Enumeration (CWE)*: The CWE was developed to document the underlying weaknesses of hardware or software systems, facilitating the identification of relevant weaknesses during software development [10], [13]. Initially, CWE started with 28 entries [10] and has since expanded to 963 entries [12]. CWE entries are organized hierarchically into pillar, class, base, and variant weaknesses, each level providing varying specificity to categorize and describe vulnerabilities. MITRE defines a “weakness” as a condition that, under specific circumstances, contributes to the introduction of vulnerabilities [13].

1) Pillar weakness: Represents the highest-level weakness, defining an abstract theme for related weaknesses [14]. Example: *CWE-682* (Incorrect Calculation) [15].

2) Class weakness: Describes an issue abstractly, independent of specific technology [16]. Example: *CWE-922* (Insecure Storage of Sensitive Information) [17].

3) Base weakness: Provides details sufficient for detecting and preventing the weakness, without specifying product type or technology [18]. Example: *CWE-22* (Improper Limitation of a Pathname to a Restricted Directory) [19].

4) Variant weakness: Linked to a specific product type or technology, providing detailed descriptions [20]. Example: *CWE-467* (Use of sizeof() on a Pointer Type) [21].

3) *Exploit Prediction Scoring System (EPSS)*: The EPSS [22] evaluates the probability of vulnerabilities being exploited. Managed by the Forum of Incident Response and Security Teams (FIRST) [23], EPSS uses statistical models and machine learning to analyze factors such as historical exploitation data and the presence of proof-of-concept exploits. Each vulnerability is assigned a score from 0 to 1, indicating the likelihood of exploitation [23]. EPSS data is continuously updated from sources like the National Vulnerability Database (NVD) [24], providing a dynamic approach to prioritizing vulnerabilities based on exploitation likelihood.

4) *Known Exploited Vulnerabilities (KEVs)*: KEVs are actively exploited by malicious actors, posing significant risks. These vulnerabilities are often found in operating systems, widely deployed applications, or network devices. Organizations like the Cybersecurity and Infrastructure Security Agency (CISA) maintain catalogs of KEVs to help prioritize security efforts [25], [26]. A notable example is the EternalBlue vulnerability (*CVE-2017-0144*) in Microsoft’s Server Message Block (SMB) protocol [27], [28], [29]. Discovered by the NSA

and leaked by the Shadow Brokers in 2017, it was exploited by the WannaCry ransomware attack, highlighting the severe impact of KEVs and the necessity for resilient cyber-reasoning systems [28], [30].

### B. Semantics

Embedding models and similarity metrics are essential for developing efficient cyber-reasoning systems. These models convert textual data into dense vector representations, facilitating advanced semantic analysis and retrieval.

1) *Embedding Models*: Embeddings represent words or entities as dense vectors in a continuous space, capturing syntactic and semantic properties such that similar items are mapped to near points in the vector space [31]. Key models include Word2Vec, GloVe, and BERT. Word2Vec, developed by Mikolov et al. [32], generates word embeddings based on contextual co-occurrences. GloVe constructs embeddings by factorizing the word co-occurrence matrix [33]. BERT uses transformer architectures to generate contextual embeddings, capturing nuanced meanings and relationships within text [2].

2) *Similarity Metrics*: Effective use of embeddings requires appropriate similarity metrics. Common metrics include cosine similarity and L2 (Euclidean) distance:

- Cosine similarity measures the cosine of the angle between two vectors, providing a value between -1 and 1. It is particularly useful for high-dimensional text data, focusing on orientation rather than magnitude [34]. It is defined as:

$$\text{Cosine Similarity} = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\| \|\mathbf{B}\|}$$

where  $\mathbf{A}$  and  $\mathbf{B}$  are vectors,  $\mathbf{A} \cdot \mathbf{B}$  denotes the dot product, and  $\|\mathbf{A}\|$  and  $\|\mathbf{B}\|$  are the magnitudes of  $\mathbf{A}$  and  $\mathbf{B}$ .

- L2 distance, also known as Euclidean distance, measures the straight-line distance between two vectors in a multidimensional space. It is effective for tasks requiring precise spatial measurements [35]. It is calculated as:

$$\text{L2 Distance} = \|\mathbf{A} - \mathbf{B}\|_2 = \sqrt{\sum_{i=1}^n (A_i - B_i)^2}$$

where  $A_i$  and  $B_i$  are the components of vectors  $\mathbf{A}$  and  $\mathbf{B}$ .

3) *Vector Databases*: Vector databases store high-dimensional vectors, enabling efficient processing and comparison using the vector space model. Examples include Facebook AI Similarity Search (FAISS) [36], a popular vector database, that enables efficient similarity search through techniques like product quantization or inverted file indexing [37] for fast approximate nearest neighbor (ANN) search. Other databases like Milvus [38] and Pinecone [39] are designed for high performance and scalability in real-time applications, making them valuable for swiftly analyzing and retrieving critical threat intelligence entries in cyber-reasoning systems [37].

### C. RAG

RAG significantly advances natural language processing (NLP) [5]. By integrating retrieval-based and generation-based methods, RAG enhances the accuracy, relevance, and richness of outputs from large language models. Traditional NLP systems either use retrieval-based methods, which are precise but limited by static data [40], or generation-based models, which can produce plausible but incorrect information [41].

RAG models combine these approaches with a retriever and a generator. The retriever uses techniques like cosine similarity and dense passage retrieval [42] to find relevant information from large external corpora. The generator then integrates this information into its outputs, improving accuracy and relevance [5].

This integration offers several benefits. RAG models efficiently handle large datasets, improving scalability and mitigating context size limitations. Grounding generation in real-world data reduces hallucinations and enhances factual accuracy [5], [41]. Additionally, RAG allows dynamic updates to knowledge bases without retraining, which is crucial for fields like cybersecurity, in which systems must adapt to new threats and vulnerabilities. Thus, RAG systems enable proactive and adaptable cyberdefense by leveraging advanced AI and database technologies.

## III. RELATED WORK

The integration of LLMs and RAG techniques in cybersecurity represents a rapidly evolving field, combining sophisticated machine learning methodologies with practical security applications. This review of the literature evaluates the leading technologies in LLM and RAG techniques for cybersecurity, examines existing frameworks, and identifies the research gaps addressed in this research.

### A. LLMs for Cybersecurity

Recent advancements in LLMs have significantly influenced the cybersecurity domain. The introduction of BERT by Devlin et al. demonstrated the efficacy of bidirectional transformers in understanding and processing security-related data [2]. BERT's deep contextual representations have been used in various cybersecurity tasks, such as threat detection and attack classification [43]. Building on this, GPT-3, introduced by Brown et al. [3], extended these capabilities with its substantial generative prowess, applied to tasks such as phishing detection [44]. GPT-3's ability for few-shot learning showed that LLMs can address diverse cybersecurity challenges with minimal task-specific training data [3]; few-shot learning is a technique in which a model learns to make accurate predictions with only a few training examples per class.

The development of GPT-4 [4] has further advanced LLM capabilities. Achiam et al. demonstrated that GPT-4 excels in handling complex and nuanced cybersecurity tasks, enhancing threat detection processes through its improved generative and contextual understanding abilities [4]. These advancements highlight the potential of LLMs in creating more versatile and effective cybersecurity tools.

### B. RAG for Cybersecurity

RAG systems, which combine external information retrieval with generative capabilities, have emerged as a novel technique to improve LLM performance. Initial research by Lewis et al. [5] showed that integrating retrieval mechanisms with generation processes significantly boosts performance across various NLP tasks by leveraging external knowledge sources. This approach has been extended to cybersecurity, where RAG systems are used to integrate threat intelligence feeds with LLMs, enhancing threat detection and response capabilities. For example, Mitra et al. [6] demonstrated the utility of RAG-based systems in generating threat reports by retrieving relevant information from external security databases. Although promising, the application of RAG systems in continuous threat intelligence feeds for real-time cybersecurity solutions remains underexplored.

### C. Continuous Threat Intelligence Feeds

Traditional cybersecurity methods, primarily reliant on signature-based detection and heuristics, face limitations in addressing new and sophisticated threats [1]. Recent studies, such as those by Hassanin et al. [45], investigated whether standard LLMs could be used for anomaly detection and incident response. The authors highlight that, while LLMs show significant potential, there is still room for improvement in their application for real-time scenarios.

In modern cybersecurity, threat intelligence feeds are crucial. Studies, such as those by Mitra et al. [6], have examined methods for integrating threat feeds into security systems, demonstrating that updates from threat intelligence sources enhance the accuracy of threat detection and response. However, there is a pressing need for approaches that incorporate continuous threat intelligence with industrial-grade LLMs and RAG techniques to develop dynamic cybersecurity solutions.

### D. Gap in the Literature: RAG-Based Continuous Threat Intelligence

Despite advancements in the application of LLMs and RAG techniques for cybersecurity, a critical gap remains: the integration of continuous threat intelligence feeds with RAG-based systems for real-time cybersecurity solutions is lacking. Existing studies primarily focus on static or batch processes rather than dynamic, continuous threat feeds [6]. This research proposes a RAG-based system leveraging continuous threat intelligence feeds to enhance real-time cybersecurity threat detection and response, addressing a crucial gap in current cybersecurity practices.

## IV. METHODOLOGY

In this section, we address the challenges identified in the literature review by implementing a methodology designed to tackle these specific issues. Our approach aims to offer practical solutions and enhance understanding in the context of the current research.

### A. Threat Intelligence Retrieval

We employed the Patrowl framework [12] to automate the retrieval of cybersecurity threat intelligence feeds. This framework efficiently processes new feed additions without reprocessing the entire dataset, ensuring streamlined updates.

1) **CVE**: Our framework accesses CVE feeds from the National Vulnerability Database (NVD) [24], using the zipped JSON format 1.1 for its efficiency and parsing ease. The automated process systematically collects all historical entries across directories organized by year, accumulating a total of 255,158 entries [12].

2) **CWE**: CWE entries, sourced from the MITRE Corporation's [cwe.mitre.org](http://cwe.mitre.org) portal [46], currently encompass 963 entries detailing both software and hardware weaknesses [12]. The original data is in CSV format, with multiple columns. For our research, we focused on the ID, name, and description of each record.

3) **EPSS**: EPSS entries, curated by the Forum of Incident Response and Security Teams (FIRST) [23] and supported by the Cyentia Institute [47], were also integrated. Typical EPSS entries include:

```

1 "CVE-2024-26604 - EPSS": {
2     "epss": "0.00042",
3     "percentile": "0.05107",
4     "date": "2024-06-28T00:00:00+0000"
5 },
6 "CVE-2004-0594 - EPSS": {
7     "epss": "0.61340",
8     "percentile": "0.97823",
9     "date": "2024-06-28T00:00:00+0000"
10 }
```

Code-Snippet 1. EPSS Example

The *epss* field quantifies the exploit prediction score, with higher values indicating increased exploitability of a given vulnerability. The *percentile* field provides a comparative measure for the exploitability of CVEs. The *date* field marks the latest update of the EPSS. For instance, the *CVE-2004-0594* vulnerability [48] remains a significant threat despite its age, contrasting with newer vulnerabilities such as *CVE-2024-26604* [49]. This underscores the necessity of considering CVE exploitability in prioritizing mitigation strategies.<sup>1</sup> Currently, FIRST has cataloged 251,953 EPSS entries [12].

4) **KEV**: CISA [25] curates a catalog of KEVs, critical for prioritizing threat mitigation. A typical KEV entry [26] includes the CVE identifier, a brief description, the affected product, and the current exploitation status, such as involvement in ransomware campaigns. CISA's repository contains 1126 KEVs to date [12]:

```

1 {
2     "cveID": "CVE-2020-4428",
3     "vendorProject": "IBM",
4     "product": "Data Risk Manager",
5     "vulnerabilityName": "IBM Data Risk Manager
6         Remote Code Execution Vulnerability",
7     "dateAdded": "2021-11-03",
8     "shortDescription": "IBM Data Risk Manager
9         contains an unspecified vulnerability which
10            could allow a remote, authenticated
```

<sup>1</sup>*CVE-2004-0594* is a vulnerability in PHP versions up to 4.3.7 and 5.0.0RC3, permitting remote code execution when *register\_globals* is enabled.

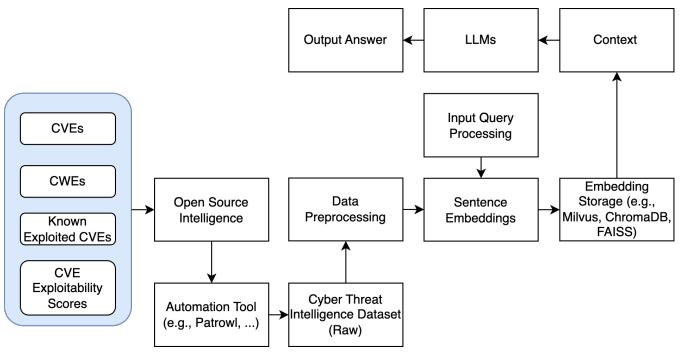


Fig. 1. Threat intelligence and user query flow

```

8     "attacker to execute commands on the
9     system.",
10    "requiredAction": "Apply updates per vendor
11       instructions.",
12    "dueDate": "2022-05-03",
13    "knownRansomwareCampaignUse": "Unknown",
14    "notes": "",
15    "cves": []
16 }
```

Code-Snippet 2. KEV Example

### B. Embeddings: Generation, Storage, and Retrieval

For generating embeddings for threat intelligence feeds, the *all-mpnet-base-v2* model [50] from the Sentence Transformers library was employed, designed for producing high-quality sentence embeddings. This model, leveraging the MPNet architecture, generates 768-dimensional dense vector embeddings, balancing computational efficiency with semantic complexity capture [50], [51].

These embeddings are stored in Milvus, an open-source vector database optimized for high-dimensional similarity searches. Milvus scales horizontally, efficiently managing extensive vector data and performing real-time searches with high accuracy and speed. It supports various index types (e.g., IVF\_FLAT [52], HNSW [53], or ANNOY [54]), balancing search precision and computational efficiency based on application needs. Additionally, Milvus's support for distributed deployments enhances performance and fault tolerance [38]. Future research is encouraged to explore distributed vector databases' efficacy in constructing large-scale cyber-reasoning systems.

User search queries are processed using the *all-mpnet-base-v2* model, converting them into vector embeddings to retain semantic meaning, as shown in Figure 1. These embeddings facilitate ANN searches in the vector database, employing cosine similarity to measure vector closeness. The vectors with the highest similarity scores are retrieved, representing the most relevant threat intelligence data. The framework ensures efficient mapping of vectors from Milvus to their original threat intelligence data points in a single database transaction. In the generation phase, these data points provide context for the user query, offering relevant information based on the semantic content.

Integrating Milvus with the all-mpnet-base-v2 model enhances the system's ability to deliver pertinent cybersecurity threat intelligence in real-time, leveraging advanced embedding generation techniques and ensuring scalability to handle large data volumes while maintaining high retrieval performance.

### C. The Generation Model

GPT-4o was selected as the generative model for the RAG system due to its proficiency in processing and generating complex domain-specific language. With a 128-k token context window [55], it adeptly handles extensive contextual inputs, making it ideal for RAG-based cybersecurity threat intelligence applications.

Upon receiving a user query, the RAG system retrieves pertinent context from the Milvus database, including detailed CVE, CWE, EPSS scores, and KEV information. This additional context allows GPT-4o to generate coherent, informative, and actionable responses.

### D. LangChain as the Synthesizer Framework

The LangChain framework [56] effectively manages complex language model pipelines, facilitating seamless integration of retrieval and generation modules in RAG systems. Its modular, extensible design is crucial for scaling and optimizing retrieval and generation processes, enhancing overall system performance [56].

LangChain's retrieval component fetches relevant documents from an extensive corpus, integrating with the Milvus vector database to streamline the process. The generative model, GPT-4o, uses these documents to produce coherent responses. LangChain coordinates the integration of these models through its generation interface.

When a user query is received, LangChain manages pre-processing steps, including tokenization and query embedding using the mpnet-base-v2 model. The embedded query is then passed to the retrieval module, ensuring the retrieval of the most relevant documents. These documents are fed into the generative model to produce a coherent response, with LangChain overseeing the incorporation of document context into generative prompts. Detailed documentation of prompts used in RAG experiments and control groups using the standard GPT-4o model is provided in the appendix. Significantly, to mitigate hallucinations, prompts are designed to instruct the models to respond with "I don't know" when uncertain about an answer.

## V. EVALUATIONS AND RESULTS

While many security tools perform source-level or binary-level analyses, these tools often incorrectly assume that cybersecurity researchers have access to the complete source code and the necessary infrastructure for thorough assessments. In practice, this is rarely the case due to proprietary restrictions or the high costs of comprehensive testing. Even with full source code access, source-level analysis can be impractically time-consuming. To address these challenges, we propose

a practical approach that minimizes resource assumptions for cybersecurity researchers and leverages a cyber-reasoning system for intensive tasks. The following case studies illustrate our approach:

**1) Recently Disclosed CVEs:** Our cyber-reasoning system significantly outperforms the vanilla GPT-4o in addressing recently disclosed vulnerabilities. Traditional models are limited to the knowledge available at the time of their training, whereas our framework continuously integrates updated threat intelligence on zero-day vulnerabilities and emerging threats. The response generated by our system regarding *CVE-2024-39471* is validated [57] and documented here:

CVE-2024-39471 is a vulnerability in the Linux kernel related to the 'drm/amdgpu' driver. The issue arises from an out-of-bounds read that can occur if the function 'sdma\_v4\_0\_irq\_id\_to\_seq' returns '-EINVAL'. To mitigate this, an error handling mechanism has been added to immediately stop the process and return '-EINVAL', thereby avoiding the out-of-bounds read.

Code-Snippet 3. CVE-2024-39471

As expected, the standard GPT-4o does not have knowledge of the CVE in question due to its training data cutoff date:

I don't have information on CVE-2024-39471. It may be a new or unreleased vulnerability, or details about it might not be publicly available yet. For the latest information, you can check the official CVE database or other trusted security resources.

Code-Snippet 4. Vanilla GPT-4o Response - CVE-2024-39471

**2) Conventional KEVs:** Regarding specific KEVs, the standard GPT-4o shows limited confidence. In contrast, our proposed framework surpasses the vanilla model by providing accurate responses. For instance, when queried about *CVE-2024-38112*, which is documented as being exploited in the wild [26], our framework was able to furnish an appropriate response:

CVE-2024-38112 is a spoofing vulnerability in the Microsoft Windows MSHTML Platform. This vulnerability has a high impact on confidentiality, integrity, and availability. The recommended action is to apply mitigations as per the vendor instructions or discontinue the use of the product if mitigations are not available. The due date for these actions is July 30, 2024. There is no known ransomware campaign using this vulnerability as of now. For more details, you can refer to the [Microsoft Security Response Center] (<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112>).

Code-Snippet 5. CVE-2024-38112

The vanilla model's response, however, remains basic:

I don't know.

Code-Snippet 6. Vanilla GPT-4o Response - CVE-2024-38112

**3) CVEs With High EPSS Scores:** Vulnerabilities with high EPSS scores are of particular importance to cybersecurity professionals due to their elevated risk and the need for prioritized mitigation. We tested the new framework to identify critical vulnerabilities with high EPSS scores for proof-of-concept (PoC) purposes [22], [12]. Here is the result from the proposed framework:

```

1 CVEs with high EPSS scores based on the
2 retrieved context are:
3
4 1. CVE-2019-16758
5   EPSS: 0.29708
6   Percentile: 0.96961
7
8 2. CVE-2006-3581
9   EPSS: 0.28304
10  Percentile: 0.96888
11
12 3. CVE-2006-0671
13   EPSS: 0.17811
14   Percentile: 0.96193
15
16 4. CVE-2004-0599
17   EPSS: 0.10541
     Percentile: 0.95061

```

Code-Snippet 7. CVEs with High EPSS Scores

And that of the vanilla LLM:

I don't have real-time access to current data, so I can't provide a list of specific CVEs with high EPSS (Exploit Prediction Scoring System) scores at this moment. However, you can find up-to-date information on CVEs with high EPSS scores by visiting the official EPSS website or related cybersecurity resources.

Code-Snippet 8. Vanilla GPT-4o Response - CVEs with High EPSS Scores

#### A. Adversarial Robustness

Adversarial robustness experiments assess how well a model handles deliberately crafted inputs designed to confuse or mislead it. We include the following robustness experiments:

- Adversarial experiments using **Misleading Vulnerability Attributes** evaluate how the model handles misleading or incorrect attributes about vulnerabilities. For instance, the original prompt could be The CVSS version 3.1 score for CVE-2024-3273 vulnerability is 9.8. An adversarial variant could be CVE-2024-3273 is categorized as a low-severity vulnerability. When targeted with the adversarial variant, the proposed framework responds as follows:

The retrieved context does not contain any information about CVE-2024-3273. Based on my knowledge, I do not have specific

details regarding the categorization of CVE-2024-3273. Therefore, I cannot confirm if it is categorized as a low-severity vulnerability. If you need accurate and detailed information, I recommend checking the official CVE database or security advisories from relevant authorities.

Code-Snippet 9. Misleading Vulnerability Attributes

As seen from the response above, the embedding model falls short of identifying the flaw in the query. As a result, non-relevant context is passed to the generator side, which in turn comes short of addressing the query. However, if we first query the framework with just the CVE entry itself (i.e., CVE-2024-3273) and provide that as a context for the aforementioned adversarial query, the model defends against the adversarial attack correctly:

The statement that CVE-2024-3273 is categorized as a low-severity vulnerability is incorrect. According to the provided context, CVE-2024-3273 is a critical vulnerability with a CVSS v3.1 base score of 9.8.

Code-Snippet 10. Misleading Vulnerability Attributes-v2

This experiment indicates that the embedding component has a room for improvement and can be made more robust with a more powerful embedding model.

- Adversarial experiments can also purposefully include **Ambiguous Queries** to test the framework's handling of vague queries pertaining to vulnerabilities. For instance, a vague query could be Tell me about CVE-2024-3273's resolution. Here is what the proposed framework has to say:

The retrieved context does not provide any information about CVE-2024-3273. Based on my own knowledge and the absence of details in the provided context, I cannot provide information on CVE-2024-3273's resolution. If you need specific details, I recommend checking the official CVE database or resources provided by the software vendor associated with the CVE.

Code-Snippet 11. Ambiguous Queries

As can be seen above, the generator complains from a lack of proper context. This is because the vague query confuses the embedding model and makes it miss the (already-present) context in the vector space. However, when we pass the correct context to the model using a chain-of-thought process, the model correctly understands the vague query:

CVE-2024-3273 is a critical vulnerability in certain D-Link

NAS devices (DNS-320L, DNS-325, DNS-327L, and DNS-340L). The resolution for this vulnerability, as indicated in the retrieved context, is as follows:

The affected products are no longer supported by the vendor and have reached their end-of-life (EOL) or end-of-service (EOS) lifecycle. The vendor has confirmed that these products should be retired and replaced. Therefore, the required action for mitigating this vulnerability is to retire and replace the affected devices according to the vendor's instructions.

For more detailed information, you can refer to the support announcement provided by D-Link: [D-Link Support Announcement] (<https://support.announcement.us.dlink.com/security/publication.aspx?name=SAP10383>).

Code-Snippet 12. Ambiguous Queries-v2

### B. Further Discussion

A key advantage of our proposed framework is its complete modularity, allowing for internal maintenance, augmentation, and replacement of individual components without affecting the overall system:

- Additional cybersecurity intelligence sources such as Feedly [58] and FireEye Threat Intelligence (now Trellix) [59] can be seamlessly integrated.
- Any embedding model that is compatible with the Sentence Transformers library API [60] can be used, including proprietary models such as `text-embedding-3` or `text-embedding-ada-002` from OpenAI [55].
- The vector database Milvus can be deployed locally, within a Docker container, in the cloud, or substituted with a different database [38].
- The generator model is flexible, supporting locally running open-source LLMs (e.g., Llama-3 70B) [61], models from the OpenAI family [55], or custom cloud deployments such as Azure [62].
- A human user can be substituted with an LLM agent, facilitating integration into a multi-agent system for fully autonomous cyber-reasoning using frameworks like Autogen [63].
- The framework supports deployment as a scheduled task or cron-job for real-time threat intelligence.

These capabilities are enabled by the modular design and the automation of the RAG mechanism via LangChain.

## VI. CONCLUSION

This research elucidates the promising integration of LLMs with RAG systems within the cybersecurity domain. Our empirical findings indicate that coupling LLMs with RAG

systems and continuous threat intelligence feeds can substantially enhance real-time threat detection and response. This integration allows for a transition from static threat analysis to a dynamic, real-time threat management paradigm, fostering a more proactive and adaptive security stance.

Furthermore, the coupling of RAG systems with continuous threat intelligence feeds, initially proposed by Mitra et al. [6] and extended in our study, offers a robust framework for using extensive external data to support automated cybersecurity decisions. This methodology addresses the shortcomings of traditional signature-based and heuristic approaches, which often falter against the swiftly evolving cyberthreat landscape [1].

Our work bridges significant gaps in current cybersecurity solutions by introducing an innovative RAG-based system that leverages continuous threat intelligence feeds for real-time application. This not only advances the role of LLMs in cybersecurity but also paves the way for future advancements in automated intelligent threat management systems. We urge the broader scientific community to build upon our findings, refine the proposed framework, and investigate advanced-prompt engineering techniques to achieve superior outcomes.

## VII. FUTURE WORKS

This paper explores the feasibility of cyber-reasoning systems driven by threat intelligence feeds through experimental validation. Further research could focus on evaluating these systems' effectiveness with tools like binary analysis frameworks and fuzzers, as well as their proficiency in navigating directories and URLs.

Future work could extend this research into a multi-agent paradigm, in which a user proxy agent communicates tasks to a managerial LLM. The LLM would divide tasks among specialized worker agents with skills in filesystem navigation, tool use, and RAG usage, ensuring high parallelizability and resilience to agent failures. The Microsoft Autogen framework [63] offers a starting point for developing such a multi-agent system.

Additionally, fine-tuning LLMs for cybersecurity and using those LLMs to generate RAG prompts shows promise. Moreover, future studies could leverage advanced embedding models from the HuggingFace Massive Text Embedding Benchmark Leaderboard [64] for more sophisticated embedding generation. Finally, the current prompts can be improved using advanced prompt engineering techniques for achieving superior results.

## ACKNOWLEDGMENTS

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported by the Laboratory Directed Research and Development Program at NREL. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government

retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

## REFERENCES

- [1] N. Idika and A. P. Mathur, "A Survey of Malware Detection Techniques," *Purdue University*, vol. 48, no. 2, pp. 32–46, 2007.
- [2] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep biDirectional Transformers for Language Understanding," *arXiv preprint arXiv:1810.04805*, 2018.
- [3] T. Brown, B. Mann, N. Ryder, M. Subbiah, J. D. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell *et al.*, "Language Models are Few-shot Learners," *Advances in Neural Information Processing Systems*, vol. 33, pp. 1877–1901, 2020.
- [4] J. Achiam, S. Adler, S. Agarwal, L. Ahmad, I. Akkaya, F. L. Aleman, D. Almeida, J. Altenschmidt, S. Altman, S. Anadkat *et al.*, "GPT-4 Technical Report," *arXiv preprint arXiv:2303.08774*, 2023.
- [5] P. Lewis, E. Perez, A. Piktus, F. Petroni, V. Karpukhin, N. Goyal, H. Küttler, M. Lewis, W.-t. Yih, T. Rocktäschel *et al.*, "Retrieval-augmented Generation for Knowledge-intensive NLP Tasks," *Advances in Neural Information Processing Systems*, vol. 33, pp. 9459–9474, 2020.
- [6] S. Mitra, S. Neupane, T. Chakraborty, S. Mittal, A. Pipali, M. Gaur, and S. Rahimi, "LOCALINTEL: Generating Organizational Threat Intelligence from Global and Local Cyber Knowledge," *arXiv preprint arXiv:2401.10036*, 2024.
- [7] OpenAI. (2024) Hello GPT-4o. Announcement of GPT-4o, a new model with enhanced audio, vision, and text capabilities. Accessed: 2024-07-08. [Online]. Available: <https://openai.com/index/hello-gpt-4o/>
- [8] MITRE Corporation, "MITRE Corporation," 2024, accessed: 2024-07-08. [Online]. Available: <https://www.mitre.org/>
- [9] MITRE Corporation - CVE, "Common Vulnerabilities and Exposures (CVE)," 2024, accessed: 2024-07-08. [Online]. Available: <https://www.cve.org/>
- [10] M. Bishop, E. Sullivan, and M. Ruppel, *Computer Security: Art and Science*, 2nd ed. Boston: Addison-Wesley, 2019, oCLC: on1076675266.
- [11] CVE, "Glossary: CNA," 2024, accessed: 2024-07-09. [Online]. Available: <https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryCNA>
- [12] Patrowl, "PatrowlHearsData," 2024, accessed: 2024-06-28. [Online]. Available: <https://github.com/Patrowl/PatrowlHearsData/tree/main>
- [13] MITRE Corporation, "Weakness - cwe glossary," 2022, accessed: 2024-07-09. [Online]. Available: <https://cwe.mitre.org/documents/glossary/#Weakness>
- [14] —, "Pillar weakness," 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/documents/glossary/#Pillar Weakness>
- [15] MITRE Corporation - CWE-682, "CWE-682: Incorrect Calculation," Common Weakness Enumeration (CWE), 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/data/definitions/682.html>
- [16] MITRE Corporation, "Class Weakness," 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/documents/glossary/#Class Weakness>
- [17] MITRE Corporation - CWE-922, "CWE-922: Insecure Storage of Sensitive Information," 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/data/definitions/922.html>
- [18] MITRE Corporation, "Base Weakness," 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/documents/glossary/#Base Weakness>
- [19] MITRE Corporation - CWE-22, "CWE-22: Improper Limitation of a Pathname to a Restricted Directory," 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/data/definitions/22.html>
- [20] MITRE Corporation, "Variant Weakness," 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/documents/glossary/#Variant Weakness>
- [21] MITRE Corporation - CWE-467, "CWE-467: Use of sizeof() on a Pointer Type," 2024, accessed: 2024-07-09. [Online]. Available: <https://cwe.mitre.org/data/definitions/467.html>
- [22] FIRST, "Exploit Prediction Scoring System (EPSS)," 2024, accessed: 2024-07-08. [Online]. Available: <https://www.first.org/epss/>
- [23] —, "The Forum of Incident Response and Security Teams," <https://www.first.org>, accessed: 2024-07-09.
- [24] National Vulnerability Database, "NVD: National Vulnerability Database," 2024, accessed: 2024-07-09. [Online]. Available: <https://nvd.nist.gov/>
- [25] Cybersecurity and Infrastructure Security Agency, "CISA: Cybersecurity and Infrastructure Security Agency," 2024, accessed: 2024-07-08. [Online]. Available: <https://www.cisa.gov/>
- [26] —, "Known Exploited Vulnerabilities Catalog," 2024, accessed: 2024-07-09. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- [27] E. Nakashima and C. Timberg, "NSA officials worried about the day its potent hacking tool would get loose..." *Washington Post*, May 2017. [Online]. Available: [https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82\\_story.html](https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html)
- [28] M. R. Gupta, "Eternal blue vulnerability," *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, no. 6, p. 1054–1060, Jun. 2023. [Online]. Available: <https://www.ijraset.com/best-journal/eternal-blue-vulnerability>
- [29] Microsoft, "MS17-010: Security Update for Microsoft Windows SMB Server (4013389)," 2017, accessed: 2024-07-08. [Online]. Available: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>
- [30] Z. Liu, C. Chen, L. Y. Zhang, and S. Gao, "Working Mechanism of Eternalblue and its Application in Ransomworm," in *International Symposium on Cyberspace Safety and Security*. Springer, 2022, pp. 178–191.
- [31] Y. Bengio, R. Ducharme, and P. Vincent, "A Neural Probabilistic Language Model," in *Advances in Neural Information Processing Systems*, T. Leen, T. Dietterich, and V. Tresp, Eds., vol. 13. MIT Press, 2000. [Online]. Available: [https://proceedings.neurips.cc/paper\\_files/paper/2000/file/728f206c2a01bf572b5940d7d9a8fa4c-Paper.pdf](https://proceedings.neurips.cc/paper_files/paper/2000/file/728f206c2a01bf572b5940d7d9a8fa4c-Paper.pdf)
- [32] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient Estimation of Word Representations in Vector Space," 2013, accessed: 2024-07-10. [Online]. Available: <https://arxiv.org/abs/1301.3781>
- [33] J. Pennington, R. Socher, and C. D. Manning, "GloVe: Global Vectors for Word Representation," in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2014, pp. 1532–1543.
- [34] C. C. Aggarwal, A. Hinneburg, and D. A. Keim, "On the Surprising Behavior of Distance Metrics in High Dimensional Space," in *Database Theory—ICDT 2001: 8th International Conference London, UK, January 4–6, 2001 proceedings 8*. Springer, 2001, pp. 420–434.
- [35] A. Huang, "Similarity Measures for Text Document Clustering," in *Proceedings of the Sixth New Zealand Computer Science Research Student Conference (NZCSRSC2008)*, Christchurch, New Zealand, vol. 4, 2008, pp. 9–56.
- [36] F. A. Research, "FAISS," <https://github.com/facebookresearch/faiss>, 2024, accessed: 2024-07-10.
- [37] J. Johnson, M. Douze, and H. Jégou, "Billion-Scale Similarity Search with GPUs," *IEEE Transactions on Big Data*, vol. 7, no. 3, pp. 535–547, 2021.
- [38] J. Wang, X. Yi, R. Guo, H. Jin, P. Xu, S. Li, X. Wang, X. Guo, C. Li, X. Xu, K. Yu, Y. Yuan, Y. Zou, J. Long, Y. Cai, Z. Li, Z. Zhang, Y. Mo, J. Gu, R. Jiang, Y. Wei, and C. Xie, "Milvus: A Purpose-Built Vector Data Management System," in *Proceedings of the 2021 International Conference on Management of Data*, ser. SIGMOD '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 2614–2627. [Online]. Available: <https://doi.org/10.1145/3448016.3457550>
- [39] Pinecone, "Pinecone," <https://www.pinecone.io/>, accessed: 2024-07-10.
- [40] D. Chen, A. Fisch, J. Weston, and A. Bordes, "Reading Wikipedia to Answer Open-Domain Questions," *arXiv preprint arXiv:1704.00051*, 2017, arXiv:1704.00051 [cs.CL]. [Online]. Available: <https://doi.org/10.48550/arXiv.1704.00051>
- [41] J. Maynez, S. Narayan, B. Bohnet, and R. McDonald, "On Faithfulness and Factuality in Abstractive Summarization," in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, D. Jurafsky, J. Chai, N. Schluter, and J. Tetreault, Eds. Online: Association for Computational Linguistics, Jul. 2020, pp. 1906–1919. [Online]. Available: <https://aclanthology.org/2020.acl-main.173>
- [42] V. Karpukhin, B. Oğuz, S. Min, P. Lewis, L. Wu, S. Edunov, D. Chen, and W.-t. Yih, "Dense passage retrieval for open-domain question answering," *arXiv preprint arXiv:2004.04906*, 2020.
- [43] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestale, and N. S. Thandi, "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices," *IEEE Access*, 2024.
- [44] F. Trad and A. Chehab, "Prompt Engineering or Fine-Tuning? A Case Study on Phishing Detection with Large Language Models," *Machine*

- Learning and Knowledge Extraction*, vol. 6, no. 1, pp. 367–384, 2024. [Online]. Available: <https://www.mdpi.com/2504-4990/6/1/18>
- [45] M. Hassanin and N. Moustafa, “A Comprehensive Overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions,” *arXiv preprint arXiv:2405.14487*, 2024.
- [46] MITRE Corporation - CWE, “Common Weakness Enumeration (CWE),” 2024, accessed: 2024-07-08. [Online]. Available: <https://cwe.mitre.org/>
- [47] Cyentia Institute, “Cyentia Institute,” 2024, accessed: 2024-07-10. [Online]. Available: <https://www.cyentia.com/>
- [48] MITRE Corporation - CVE-2004-0594, “CVE-2004-0594,” <https://www.cve.org/CVERecord?id=CVE-2004-0594>, 2004, accessed: 2024-07-10.
- [49] MITRE Corporation - CVE-2024-26604, “CVE-2024-26604,” <https://www.cve.org/CVERecord?id=CVE-2024-26604>, 2024, accessed: 2024-07-10.
- [50] H. Face, “all-mpnet-base-v2,” <https://huggingface.co/sentence-transformers/all-mpnet-base-v2>, 2024, accessed: 2024-07-10.
- [51] N. Reimers and I. Gurevych, “Making Monolingual Sentence Embeddings Multilingual using Knowledge Distillation,” in *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 11 2020. [Online]. Available: <https://arxiv.org/abs/2004.09813>
- [52] H. Jegou, M. Douze, and C. Schmid, “Product Quantization for Nearest Neighbor Search,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 1, pp. 117–128, 2010.
- [53] Y. A. Malkov and D. A. Yashunin, “Efficient and Robust Approximate Nearest Neighbor Search Using Hierarchical Navigable Small World Graphs,” *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, vol. 42, no. 4, pp. 824–836, 2020. [Online]. Available: <https://doi.org/10.1109/TPAMI.2018.2889473>
- [54] Spotify, “ANNOY (Approximate Nearest Neighbors Oh Yeah),” 2024, accessed: 2024-07-10. [Online]. Available: <https://github.com/spotify/annoy>
- [55] OpenAI, “Models - OpenAI Platform,” <https://platform.openai.com/docs/models>, 2024, accessed: 2024-07-10.
- [56] LangChain, “LangChain,” <https://www.langchain.com/>, accessed: 2024-07-12.
- [57] MITRE Corporation - CVE-2024-39471, “CVE-2024-39471,” <https://www.cve.org/CVERecord?id=CVE-2024-39471>, 2024, accessed: 2024-07-10.
- [58] Feedly, “Feedly for Threat Intelligence,” accessed: 2024-07-10. [Online]. Available: <https://feedly.com/threat-intelligence>
- [59] Trellix, “Advanced Cyber Threat Services: Threat Intelligence Services,” <https://www.trellix.com/services/advanced-cyber-threat-services/threat-intelligence-services/>, 2024, accessed: 2024-07-10.
- [60] N. Reimers and I. Gurevych, “Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks,” in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 11 2019. [Online]. Available: <https://arxiv.org/abs/1908.10084>
- [61] Meta, “Meta Llama-3-70B,” <https://huggingface.co/meta-llama/Meta-Llama-3-70B>, 2023, accessed: 2023-10-17.
- [62] Microsoft, “AI Solutions,” <https://azure.microsoft.com/en-us/solutions/ai>, 2023, accessed: 2024-07-10.
- [63] Q. Wu, G. Bansal, J. Zhang, Y. Wu, S. Zhang, E. Zhu, B. Li, L. Jiang, X. Zhang, and C. Wang, “AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation,” *arXiv preprint arXiv:2308.08155*, 2023.
- [64] Hugging Face, “MTEB Leaderboard,” <https://huggingface.co/spaces/mteb/leaderboard>, 2023, accessed: 2023-10-12.

## APPENDIX

*Appendix A**Proposed Framework Query-Prompt: System Prompt*

```

1 """You are an assistant specializing in question-answering tasks. Use the provided context to answer the
2   question. If the context does not contain the answer, rely on your own knowledge. If you are still NOT
3   very sure of your answer, just say "I don't know"; DO NOT GUESS.
4
5 Question: {question}
6 Context: {context}
7 Answer:
8 """

```

Code-Snippet 13. Proposed Framework Query-Prompt

*Vanilla GPT-4o Query-Prompt: System Prompt*

```

1 """You are an assistant specializing in question-answering tasks. Use your own knowledge to answer the
2   question. If you are NOT very sure of your answer, just say "I don't know"; DO NOT GUESS.
3
4 # Question: {question}
5 # Answer:
6 """

```

Code-Snippet 14. Vanilla GPT-4o Query-Prompt