



Aetheria: A multimodal interpretable content safety framework based on multi-agent debate and collaboration

Yuxiang He^{a,b,1,2}, Jian Zhao^{a,1}, Yuchen Yuan^a, Tianle Zhang^a, Wei Cai^{a,c},
Haojie Cheng^{a,d}, Ziyan Shi^{a,e}, Ming Zhu^f, Haichuan Tang^f, Chi Zhang^a, Xuelong Li^{a,*}

^a*Institute of Artificial Intelligence (TeleAI), China Telecom, Beijing, China*

^b*Sichuan University, Chengdu, China*

^c*Peking University, Beijing, China*

^d*Beijing Jiaotong University, Beijing, China*

^e*Harbin Institute of Technology, Harbin, China*

^f*China Railway Rolling Stock Corporation Limited, Beijing, China*

Abstract

The exponential growth of digital content presents significant challenges for content safety. Current moderation systems, often based on single models or fixed pipelines, exhibit limitations in identifying implicit risks and providing interpretable judgment processes. To address these issues, we propose Aetheria, a multimodal interpretable content safety framework based on multi-agent debate and collaboration. Employing a collaborative architecture of five core agents, Aetheria conducts in-depth analysis and adjudication of multimodal content through a dynamic, mutually persuasive debate mechanism, which is grounded by RAG-based knowledge retrieval. Comprehensive experiments on our proposed benchmark (AIR-Bench) validate that Aetheria not only generates detailed and traceable audit reports but also demonstrates significant advantages over baselines in overall content safety accuracy, especially in the identification of implicit risks. This framework establishes a transparent and interpretable paradigm, significantly advancing the field of trustworthy AI content moderation.

Keywords: Content safety, Multi-agent systems, Interpretable AI, Multimodal

*Corresponding author.

Email address: xuelong_li@chinatelecom.cn (Xuelong Li)

¹Both authors contributed equally to this research.

²Work done during an internship at TeleAI.

1. Introduction

The exponential growth of digital content, driven mainly by social networks and generative AI, has presented significant challenges to content safety [1, 2]. The increasingly complex input contents not only make the traditional simple filtering of explicit content violation (*e.g.* violence, hate speech) insufficient, but also raise higher demands for identifying deep-seated, implicit risks. Current multimodal models, despite their visual capabilities, often exhibit a significant gap in understanding social nuances and human behavior metaphors [3]. These include cultural biases, value misguidance, and subtle discrimination, which often evade detection by standard classifiers [4, 5, 6, 7]. Fostering a truly healthy and trustworthy digital ecosystem requires addressing these nuanced threats [8, 9, 10, 11].

In practice, however, most existing content safety frameworks exhibit limitations. Traditional frameworks based on keyword matching or shallow machine learning classifiers struggle with contextual semantic understanding [12, 13]. They are particularly inadequate in processing multimodal content and are brittle against simple adversarial obfuscations [14, 15, 16].

On the other hand, deep learning or Large Language Model (LLM) based frameworks have made considerable advances in performance. However, they typically function as “black-box” systems [17, 18], making their decision-making processes hard to trace or audit. More importantly, these monolithic systems inevitably suffer from single-model biases and hallucinations [19, 20, 21]. They often demonstrate insufficient capability in identifying implicit risks that require deep reasoning and diverse cultural contextual knowledge [22], failing to meet the dual requirements of comprehensiveness and interpretability [23, 24].

As illustrated in table 1, existing paradigms often fail to simultaneously satisfy the critical requirements of implicit risk detection, interpretability, and multimodal grounding. For high-stakes tasks, providing the moderation reason (legitimacy) is as critical as the moderation result itself [25, 26].

Table 1: **Comparison with Existing Paradigms.** Aetheria uniquely integrates adversarial debate and RAG-based grounding. (Symbols: ✓ Strong, ● Partial, ✗ None)

Capability	Traditional API (e.g. Azure API)	Safety Models (e.g. Llama Guard)	Aetheria (Ours)
Multimodal Input	●	●	✓
Implicit Risk Detection	✗	●	✓
Explainability	✗	●	✓
Adversarial Mechanism	✗	✗	✓
Knowledge Grounding	✗	✗	✓

In this paper, to address the aforementioned issues, we propose Aetheria³, a multimodal interpretable AI content safety framework based on multi-agent debate and collaboration. The name ‘Aetheria’ is inspired by the concept of a ‘heavenly and purified land,’ which reflects our goal of establishing a robust content safety framework. Our core contributions are listed below:

- We propose Aetheria, a novel multimodal interpretable content safety framework based on multi-agent collaboration. It employs five specialized AI agents (Preprocessor, Supporter, Strict Debater, Loose Debater, and Arbiter) working in concert. This architecture enables a nuanced, multi-faceted analysis of complex content, significantly surpassing the depth and interpretability of single-model baselines
- We design a grounded dialectical reasoning mechanism to discern implicit risks. Unlike generic debate systems, we construct a specific philosophical clash between a Strict Debater (prioritizing objective risk and bottom-line safety) and a Loose Debater (advocating for contextual exoneration and benign intent). This adversarial dynamic effectively surfaces subtle threats like cultural biases that typically evade detection when context is ignored.

³The code and dataset are available at <https://github.com/Herrieson/Aetheria>.

- The framework achieves transparent decision-making via a Hierarchical Adjudication Protocol. The Arbiter does not merely aggregate scores but enforces a structured logic that weighs validated risks against proven benign contexts to generate a comprehensive audit report. By integrating the Preprocessor’s visual-to-text translation, Aetheria extends this high-level interpretability to multimodal content, ensuring decisions are traceable and trustworthy.
- We construct AIR-Bench, a challenging multimodal benchmark specifically targeting implicit semantic risks. Extensive experiments demonstrate that Aetheria significantly outperforms baselines, with ablation studies validating the critical roles of the RAG-based grounding and the adversarial debate mechanism.

2. Related Work

This section reviews the evolution of content safety and the key technologies that ground the design of Aetheria. We first examine traditional and deep learning-based moderation methods (Section 2.1-2.2), followed by the foundations of multi-agent systems and explainable AI (Section 2.3-2.4), and finally define the specific research gap (Section 2.5) that our framework addresses.

2.1. Traditional Content Safety Methods

Early content safety approaches predominantly relied on deterministic and statistical methods. Rule-based systems, such as keyword blocklists and regular expressions, were widely adopted for their simplicity and high inference speed [13, 27]. Subsequently, traditional machine learning classifiers, including Naive Bayes and Support Vector Machines (SVMs) trained on n-gram features, were introduced to handle more diverse text classifications [28].

While effective for detecting explicit and blatant violations, these methods lack deep semantic understanding. They struggle with contextual ambiguity, such as distinguishing varying semantics of sensitive words in gaming versus threatening contexts, and are brittle against adversarial obfuscations like “leetspeak” or deliberate misspellings [14, 16]. Consequently, they are often incapable of identifying implicit,

non-obvious risks, such as subtle cultural biases or harmful insinuations, which require nuanced comprehension[9, 11].

2.2. Deep Learning-based Content Moderation

The advancement of deep learning, particularly the emergence of Large Language Models (LLMs) and Multimodal Large Language Models (MLLMs), has significantly transformed content moderation. Transformer-based architectures have demonstrated superior performance by capturing complex semantic contexts and cross-modal interactions [29, 7]. Recent works have further leveraged the reasoning capabilities of LLMs to perform zero-shot or few-shot safety auditing [30].

However, relying solely on single-model LLMs introduces significant challenges. First, despite their performance, they largely function as “black boxes”. A model may output a safety score, but often fails to provide a rigorous, traceable justification for its decision, limiting transparency and auditability [31, 18]. Second, single models suffer from inherent biases and hallucination issues. Their judgments reflect a monolithic perspective, making them unreliable for identifying subtle, implicit risks that require multi-faceted reasoning [20, 19].

Our work, on the other hand, directly addresses the two issues of interpretability and single-model bias.

2.3. Multi-Agent Systems (MAS)

Multi-agent systems (MAS) have achieved remarkable success in solving complex tasks by decomposing them into sub-problems handled by specialized, collaborative agents. This paradigm has been effectively applied in domains ranging from software development [32, 33] to complex reasoning tasks [34, 23].

A key advantage of MAS is its ability to handle ambiguity through structured interaction. By assigning distinct roles (*e.g.* proposer, verifier), agents can simulate a “Society of Minds”, where diverse perspectives contribute to a more comprehensive solution [23, 35]. While MAS has been explored for general reasoning, its specific application to interpretable multimodal content safety, particularly for detecting implicit risks via adversarial collaboration, remains an emerging area of research.

2.4. Explainable AI (XAI) and Debate Systems

The demand for trustworthy AI has driven the development of Explainable AI (XAI). While intrinsic explainability methods like Chain-of-Thought (CoT) prompting [22] expose a model’s reasoning steps, a single CoT path is prone to unverified errors or “sycophancy,” defined as the tendency to align with user misconceptions rather than objective truth [36, 37].

To address this, recent research has proposed multi-agent debate as a robust mechanism for truth-seeking. Studies have shown that encouraging multiple LLM instances to debate and critique each other’s responses significantly improves factuality and reasoning consistency [23, 35]. In this context, the process of the debate, comprising arguments, counter-arguments, and convergence, serves as a natural, human-readable explanation. Aetheria adopts this “explanation-by-debate” principle to ensure that safety judgments are not only accurate but also fully transparent.

Most recently, this paradigm has been extended to safety evaluation. Lin et al. [38] demonstrated that an adversarial debate between “Critic” and “Defender” agents enables small models to efficiently detect jailbreak attacks. However, their framework primarily employs debate as a means to enhance binary classification accuracy within textual interactions, relying solely on the models’ internal parametric knowledge.

Aetheria significantly distinguishes itself by evolving this paradigm into a grounded dialectical reasoning framework for multimodal intent discernment. Unlike ungrounded adversarial setups, our architecture instantiates a philosophical clash between “Strict Risk Confirmation” and “Contextual Exoneration”, anchored by retrieved historical precedents (RAG). By empowering a Loose Debater to advocate for benign context (*e.g.* educational intent) against a Strict Debater’s scrutiny using factual case evidence, Aetheria simulates the nuanced cognitive process of a human auditor. This approach ensures that the final judgment is not merely a probability score, but a transparent verdict derived from resolving the tension between objective risk and contextual nuance, particularly in complex cross-modal scenarios where visual and textual cues conflict.

2.5. Research Gap

The reviewed literature reveals an important yet unaddressed research gap. Traditional methods (Section 2.1) fail on semantic context understanding. Deep learning models (Section 2.2) improve context understanding, but lack interpretability and are susceptible to single-model bias, especially for implicit risks. MAS (Section 2.3) offer a collaborative paradigm, but have not yet been prevalently applied to this moderation niche. Finally, agent-based debate (Section 2.4) presents a promising path toward robust, intrinsic explainability.

Therefore, a framework that synthesizes these advances is highly favorable: one that adopts a multi-agent debate architecture to explicitly address the implicit, multimodal risks that current black-box systems are unable to, and generate a fully transparent and interpretable audit trail. We thus design the Aetheria framework to fill this research gap.

3. The Aetheria Framework

3.1. Overview

The Aetheria framework adopts a multi-agent architecture with five specialized agents working in concert. Figure 1 illustrates the complete system architecture and information flow.

3.2. Core Agent Design

To handle diverse input modalities effectively, Aetheria employs an *adaptive prompting strategy*. Depending on the input type (Text-only, Image-only, or Multimodal), the agents are dynamically initialized with specialized instruction sets, ensuring that the debate focuses on relevant dimensions (*e.g.* visual hazard elements for images versus jailbreak patterns for text).

3.2.1. Preprocessor

As the framework’s entry point, the Preprocessor’s core responsibility is to parse raw user input and standardize potentially multimodal content (*e.g.* text, images) into a

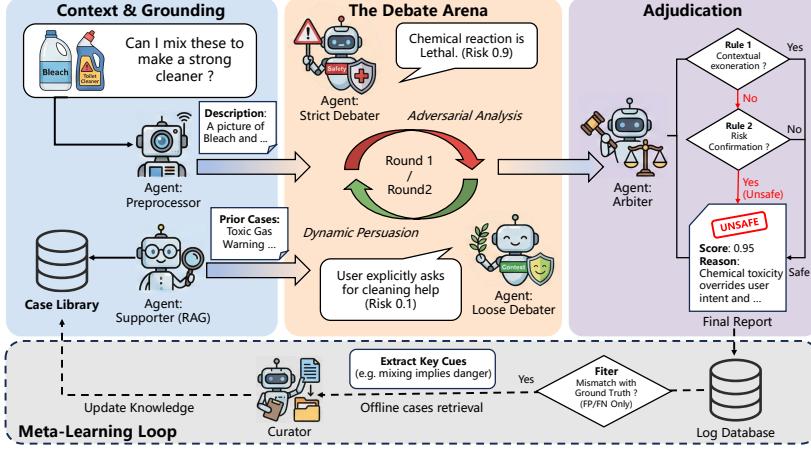


Figure 1: Overview of the Aetheria Framework Architecture. The pipeline consists of three online phases and one offline loop: (1) **Context & Grounding**, where multimodal inputs are standardized by the Preprocessor and grounded with historical precedents via the Supporter (RAG); (2) **The Debate Arena**, which facilitates an adversarial multi-round dialogue between a risk-averse Strict Debater and a context-aware Loose Debater; (3) **Adjudication**, where the Arbiter derives a transparent verdict using a Hierarchical Adjudication Protocol. Additionally, an offline Meta-Learning Loop continuously refines the Case Library by retrieving samples from the Log Database and extracting key cues to improve future reasoning.

uniform, text-only format. By utilizing an integrated Vision-Language Model (VLM) to translate the input image into a detailed, objective textual description, the Preprocessor ensures that all subsequent analytical agents (*e.g.* Debaters, Arbiter) operate on a consistent data stream. We also incorporate a robustness-oriented mechanism: in cases of VLM failure or if the image modal is deactivated, the system generates a neutral placeholder text. This ensures the consistency of the moderation pipeline and prevents process interruption due to input parsing failures.

3.2.2. *Supporter*

The Supporter provides essential external context and historical knowledge via a Retrieval-Augmented Generation (RAG) mechanism. Its role involves a multi-step analytical process rather than simple retrieval. First, the agent constructs a concise summary of the current input to serve as an analytical baseline. Second, it queries the knowledge base to retrieve the Top- K most relevant historical precedents. Third, in-

stead of merely listing cases, it analyzes them to extract key risk cues and explicitly notes critical differences (*e.g.* differing intents or contexts) between the historical cases and the current input. Finally, the Supporter identifies and reports any observed patterns, such as recurring risk categories. This comprehensive briefing serves to ground the subsequent debate in relevant, data-driven historical context.

3.2.3. Strict Debater

The Strict Debater is responsible for conducting an adversarial analysis from a rigorous, risk-averse perspective. Configured to represent the “bottom line” of safety policies, it adopts a worst-case interpretation strategy. Its primary function is to proactively identify *objective* risk elements within the content (*e.g.* weapons in images, malicious code in text) and potential jailbreak patterns, explicitly prioritizing these objective hazards over the user’s stated benign intent.

The debate process is configured as a fixed 2-round adversarial exchange. In each round, the Strict Debater evaluates its opponent’s arguments, the Supporter’s background knowledge, and its own previous assessment. It generates a detailed analysis accompanied by a Risk Score (S), where $S \in [0.0, 1.0]$ (1.0 indicating extreme risk). A score fallback logic ensures stability: if a score cannot be extracted, a default value (0.5 for the first round, previous score for subsequent rounds) is applied.

3.2.4. Loose Debater

As the counterpart to the Strict Debater, the Loose Debater simulates the perspective of a naive user or a defense attorney. Rather than simply refuting arguments, its core directive is to identify Contextual Exoneration. It analyzes the input to determine if the user’s intent is benign (*e.g.* educational inquiry, artistic expression, or news reporting) and whether the visual context supports this harmless interpretation. It is explicitly instructed to raise its risk score *only* when new, compelling evidence of harm emerges that cannot be explained by a safe context. This adversarial design compels the Strict Debater to prove that the risk is real and actionable, not just hypothetical.

3.2.5. Arbiter

The Arbiter serves as the final judge, transforming the debate logs and score trajectories into a decisive, interpretable verdict. Unlike traditional methods that simply aggregate scores, the Arbiter employs a structured Hierarchical Adjudication Protocol to resolve conflicts. As illustrated in our system design, it follows a strict priority-based decision logic:

1. **Rule 1: Contextual Exoneration (Fix False Positives).** The Arbiter first verifies if the Loose Debater has provided sufficient evidence of a benign context (*e.g.* an explicit AI refusal in the input, or a clear educational scenario) that overrides objective risk indicators. If verified, the content is deemed Safe.
2. **Rule 2: Risk Confirmation (Catch False Negatives).** If no exemption applies, it checks if the Strict Debater has identified concrete violations of safety policies (*e.g.* actionable harm instructions or hate symbols). If such evidence exists, the content is deemed Unsafe.
3. **Rule 3: Default Safety.** For ambiguous cases where neither concrete harm nor clear benign context is dominant, the system defaults to a Safe judgment to avoid over-suppression.

This logic ensures that the final judgment is not just a mathematical average but a reasoned decision. The Arbiter outputs a Final Judgment and a Final Score (following the same 0.0-1.0 metric), citing specific evidence from the debate to justify which rule was applied.

3.3. Multimodal Tool Pool

This component serves as the technical foundation for Aetheria’s multimodal processing, primarily providing the Preprocessor agent with its core analytical tools. Its key responsibility within the current framework is to supply a state-of-the-art Vision-Language Model (VLM) when the Preprocessor receives multimodal content. This VLM performs feature extraction by “translat[ing] the input image into a detailed, objective textual description”. This standardization process is critical, as it converts all

inputs into a “uniform, text-only format”. This design ensures that the subsequent debate agents (Strict Debater, Loose Debater) and the Arbiter operate on a consistent data stream, enabling them to “debate” the implicit risks within visual content.

3.4. Memory and Continuous Learning Component

To enable the framework to evolve through experience, we design a Memory and Continuous Learning Component that functions as an offline meta-learning loop. This mechanism is triggered asynchronously after the completion of an online evaluation phase. It automatically retrieves “failed cases”, specifically False Positives (FP) and False Negatives (FN), from the Log Database where the predicted verdict of Aetheria diverged from the ground truth.

As illustrated in Figure 1, the core of this process is the Curator, a specialized component designed for post-mortem analysis. Crucially, the Curator operates in a “white-box” setting with full access to both the ground truth labels and the historical debate logs. Unlike the online debate agents who must infer safety from scratch, the primary role of the Curator is explanatory and extractive. It identifies the specific logical divergence between the debate trajectory and the correct outcome, effectively performing a hindsight analysis. Given that the Curator generates insights based on known answers rather than performing open-ended prediction, the reasoning complexity is minimized. This ensures stability and low bias using a single strong instruction-following model (GPT-4o).

The Curator distills these findings into structured “Key Cues”, such as specific visual patterns or rhetorical traps, along with a concise “Summary.” This distilled knowledge is then integrated back into the Case Library. Consequently, the Supporter agent can leverage these “lessons learned” from past errors as domain priors in future tasks, enabling continuous and iterative performance optimization without parameter updates.

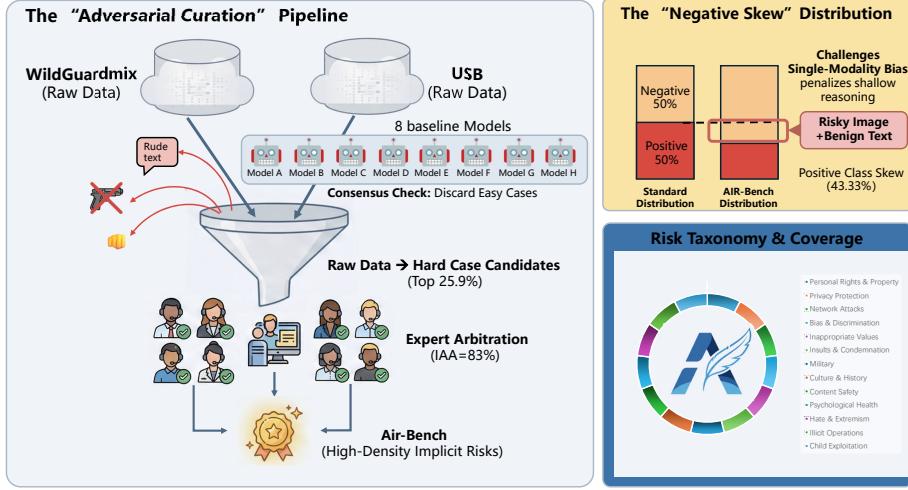


Figure 2: **Overview of the AIR-Bench Construction and Statistics.** (a) **Adversarial Curation Pipeline:** The data undergoes a rigorous “Difficulty Screening” by 8 baseline models followed by expert arbitration. (b) **Negative Skew Distribution:** We intentionally introduce a positive class skew (43.33%) to penalize single-modality bias. (c) **Risk Taxonomy:** The benchmark covers 12 distinct risk categories including Bias, Hate, and Network Attacks.

4. Experiments and Evaluation

4.1. Experimental Setup

4.1.1. Dataset

To evaluate the Aetheria framework, especially its capability in identifying implicit risks, we construct a specialized benchmark dataset AIR-Bench (Aetheria Implicit Risk Benchmark). Diverging from conventional datasets that concentrate on explicit risks (*e.g.* overt violence or hate speech), AIR-Bench is composed of complex user queries directed at AI systems, wherein the associated risks are typically subtle and non-obvious.

Our dataset is curated from two sources: WildGuardmix [39] and the USB (Unified Safety Evaluation Benchmark) [40]. These sources are selected for their renown in providing diverse, real-world adversarial prompts and edge cases.

To ensure annotation quality and specifically target the evaluation of implicit risks, we do not use the original labels directly. Instead, we implement a multi-stage annota-

tion refinement pipeline:

1. **Difficulty Screening:** We first employ eight baseline models (*e.g.* Grok-3, DeepSeek-V3.1) to conduct a preliminary analysis of the raw data. If a model’s analysis diverges from the original label, or inter-model disagreement occurs, the corresponding data sample is flagged as a “difficult/ambiguous case.”
2. **Expert Arbitration:** All samples flagged as “difficult/ambiguous cases” (comprising approximately 25.9% of the total data) are adjudicated by a human expert team consisting of two senior domain experts and one graduate researcher. To ensure rigorousness, we employ a custom-developed “human-in-the-loop” annotation toolkit. This tool enforces a strict review protocol: it simultaneously renders the high-resolution image and text query, requiring experts to explicitly evaluate the multimodal context before casting independent votes. This mechanism prevents “text-only bias” in human annotation and ensures high inter-annotator agreement (IAA = 83%), demonstrating a high level of consistency in adjudicating these complex implicit risks.

The final dataset contains 3,274 samples with the following distribution:

- **Modality Distribution:** 1,000 text samples, 988 image samples, and 1286 image-text pair samples.
- **Label Distribution:** The proportion of samples adjudicated as “risky” varies by modality: 50% of text-only samples, 48.68% of image-only samples, and 43.23% of image-text pair samples are labeled as “risky”.

A noteworthy characteristic is the negative class skew in the image-text modality (43.23% risky), which is a deliberate design choice. Real-world multimodal content is often contextually complex; for instance, a visually sensitive image (*e.g.* a bomb) may be paired with benign text (*e.g.* an inquiry about its history). Many baseline models exhibit “single-dimension bias”, flagging such content as risky based on the image alone, leading to high recall but very low precision. To penalize this tendency for “indiscriminate positive judgments” and specifically reward models capable of deep, cross-modal

contextual reasoning, the benchmark intentionally incorporates a larger proportion of these challenging negative samples. While we ensure most samples require holistic analysis, the skew towards the negative class serves as a critical mechanism to challenge models that lack true multimodal understanding.

We therefore posit that the overall performance on this benchmark directly reflects a model’s capability to identify implicit risks. A model incapable of effectively addressing these expert-validated implicit threats is unlikely to achieve a high score on this benchmark.

Knowledge Base Initialization. To address the “cold start” challenge in the RAG component and ensure the Supporter agent is functional at the start of evaluation ($T = 0$), we construct an initialized seed case library. We select 3,000 residual samples from the source datasets (WildGuardmix and USB), which will be excluded from the AIR-Bench test set. These samples share a homologous distribution with the AIR-Bench to ensure retrieval relevance, yet remain strictly non-overlapping to prevent data leakage. To populate the library, we conduct an offline bootstrapping process: the framework first processes these samples in a “cold-start” mode (i.e., without retrieval). The Curator component then analyzes the resulting execution logs against the ground truth to extract high-quality “Key Cues” and reasoning patterns. This setup simulates a realistic “warm-start” scenario where the system possesses domain priors, guaranteeing that the evaluation reflects the framework’s reasoning capability on unseen data rather than a lack of basic knowledge.

4.1.2. Baseline Models

To comprehensively evaluate the performance of the Aetheria framework, we select three representative categories of baselines for comparison. All local open-source models are obtained from the Hugging Face platform.

Commercial APIs. OpenAI Moderation and Azure Content Safety are adopted in our experiments. We utilize the `omni-moderation-latest` version of OpenAI Moderation, which returns a final, comprehensive safety determination. For Azure Content Safety, it returns severity levels (0, 2, 4, 6) for various safety categories (e.g. Hate,

Self-harm). We establish a threshold: content is classified as Harmful if the severity score in any category is ≥ 2 . This threshold (2) is selected as the optimal value through experimental tuning.

Local Open-Source Models. We employ ShieldGemma-9B, ShieldLM-6B-chatglm, and Vicuna-7B as our open-source baselines, with few-shot inference adopted. Specifically, we provide four randomly sampled examples (including both positive and negative cases) along with detailed judgment criteria within the prompt to guide the model’s safety decisions. For llama-1B-guard, as its architecture does not support few-shot prompting, we adhere to its official recommended usage (via Hugging Face): the content under inspection is directly fed into the model, and we parse its final returned result.

Multimodal Handling. The aforementioned text-only local models (ShieldGemma-9B, ShieldGemma-2B, ShieldLM-6B-chatglm, Vicuna-7B, and llama-1B-guard) are incapable of directly processing visual data. To ensure a fair comparison of reasoning capabilities, we strictly align the input processing of these baselines with Aetheria’s pipeline. Adopting the identical mechanism described in the Multimodal Tool Pool (Section 3.3), we employ the same advanced Vision-Language Model (GPT-4.1) to generate detailed textual descriptions for all visual inputs. This standardization ensures that both Aetheria and the baselines operate on the same semantic information, effectively isolating the contribution of our multi-agent debate framework from the raw visual perception capabilities. Subsequently, this generated description—or a combination of the description and the original text in the case of mixed content—is provided to the text-based models for the final safety assessment.

4.1.3. Evaluation Metrics

We adopt precision (P), recall (R), and F1 Score as evaluation metrics. The “Harmful” category is designated as the positive class. During our experiments, some models occasionally produce unparseable or anomalous outputs (*e.g.* error messages or malformed formats). To ensure a fair and accurate evaluation, these invalid samples are excluded from the final metric computation.

Table 2: Performance comparison between Aetheria and baseline models on AIR-Bench. The best results are highlighted in bold.

Model	Text Only			Image Only			Text + Image		
	P	R	F1	P	R	F1	P	R	F1
ShieldGemma-9B	0.88	0.93	0.90	0.94	0.72	0.82	0.66	0.84	0.74
ShieldGemma-2B	0.85	0.89	0.87	0.90	0.61	0.73	0.66	0.88	0.75
ShieldLM-6B-chatglm	0.94	0.68	0.79	0.51	0.97	0.67	0.44	0.99	0.61
Vicuna-7B	0.80	0.92	0.85	0.57	0.76	0.65	0.67	0.56	0.61
llama-1B-guard	0.55	0.96	0.70	0.53	0.74	0.62	0.48	0.88	0.62
Aetheria (Ours)	0.92	0.91	0.92	0.90	0.85	0.87	0.83	0.85	0.84
Azure Content Safety	0.85	0.40	0.55	0.73	0.15	0.25	0.72	0.46	0.50
OpenAI Moderation	0.87	0.46	0.60	0.74	0.17	0.28	0.81	0.67	0.73

4.2. Results and Analysis

4.2.1. Overall Performance

Table 2 presents a detailed performance comparison between Aetheria and mainstream baseline models on our proposed dataset AIR-Bench. As described in Section 4.1.1, this dataset is primarily composed of complex user queries fed to AI models that require deep reasoning and contextual understanding, where the risks contained are generally *implicit* rather than explicit.

- **Multimodal (Text+Image) Task.** This task represents the most challenging scenario in our benchmark. Aetheria achieves a superior F1 score of **0.84**, significantly outperforming the best baseline ShieldGemma-2B (0.75 F1). In particular, while some baselines like ShieldLM-6B achieve near-perfect recall (0.99), their precision is unacceptably low (0.44), indicating a tendency to aggressively flag safe content as risky. Aetheria, however, maintains high recall (0.85) while achieving the highest precision (0.83) among all models. On the other hand, commercial APIs such as Azure Content Safety struggle significantly with this task (only 0.50 F1). Their low recall (0.46) suggests that black-box

models trained primarily on explicit violations fail to capture the subtle, context-dependent risks inherent in multimodal inputs.

- **Text-Only Task.** Aetheria continues to thrive on the text-only task with an F1 score of **0.92**. While ShieldGemma-9B remains competitive (0.90 F1), Aetheria achieves an even better balance of precision (0.92) and recall (0.91). In contrast, the commercial baseline Azure exhibits a severe drop in recall (0.40), exacerbating the observation that conventional safety filters are overly conservative and rigid when handling implicit textual cues that require reasoning.
- **Image-Only Task.** Aetheria achieves an F1 score of **0.87**, outperforming the best baseline ShieldGemma-9B (0.82 F1). It is worth noting that ShieldLM-6B-chatglm again exhibits extreme behavior, *i.e.* high recall (0.97) but poor precision (0.51), further validating the necessity of Aetheria’s debate mechanism. The debate process allows the Strict Debater to flag potential risks while the Loose Debater filters out false positives, resulting in a robust and balanced system capable of interpreting subtle visual biases or improper implications.

In summary, Aetheria demonstrates consistent superiority across all modalities. It effectively solves the “high recall, low precision” dilemma faced by many open-source models and the “low recall” issue being typical in commercial APIs, proving the robustness of the multi-agent debate framework in identifying complex implicit risks.

4.2.2. *Ablation Study*

To validate the effectiveness of each key component within the Aetheria framework, we conduct a comprehensive ablation study, which involves three dimensions: (1) the effectiveness of the RAG Supporter module; (2) the composition strategy of the agent backbone models; and (3) the design of the multi-agent debate mechanism. All experimental results are aggregated in Table 3.

Analysis of RAG Module Necessity. We evaluate the impact of external knowledge by removing the RAG retrieval function and the Supporter agent entirely.

Table 3: Ablation study of the Aetheria framework’s core components based on updated experimental data. We report precision (P), recall (R), and F1 score. The best performance in each category is marked in **bold**.

Configuration	Text Only			Image Only			Text + Image		
	P	R	F1	P	R	F1	P	R	F1
Full Model	0.92	0.91	0.92	0.90	0.85	0.87	0.83	0.85	0.84
<i>RAG Module</i>									
w/o RAG Retrieval	0.94	0.88	0.91	0.89	0.84	0.86	0.86	0.75	0.80
w/o Supporter Agent	0.93	0.87	0.90	0.83	0.83	0.83	0.90	0.70	0.79
<i>Model Composition</i>									
All GPT-4o	0.93	0.89	0.91	0.94	0.62	0.75	0.82	0.85	0.84
All GPT-4o-mini	0.91	0.92	0.92	0.75	0.95	0.84	0.76	0.86	0.81
<i>Debate Mechanism</i>									
w/o Loose Debater	0.91	0.92	0.92	0.94	0.65	0.77	0.77	0.90	0.83
w/o Strict Debater	0.95	0.86	0.90	0.90	0.76	0.82	0.86	0.80	0.83
Arbiter Only (No Debate)	0.98	0.78	0.87	0.60	0.96	0.74	0.57	0.88	0.70

- **Impact on Multimodal Tasks:** As shown in Table 3, removing RAG capabilities leads to a notable performance drop in the complex Text + Image task. The F1 score decreases from 0.84 (Full) to 0.80 (w/o RAG) and further to 0.79 (w/o Supporter).
- **Recall Decline:** Specifically, the recall for multimodal inputs drops significantly (from 0.85 to 0.75/0.70). This indicates that without the Supporter providing context on potentially harmful symbols or obscure references, the system fails to recognize implicit risks that span across modalities.

Analysis of Heterogeneous Model Composition. We compare our heterogeneous backbone strategy against homogeneous setups (All GPT-4o and All GPT-4o-mini). The results challenge the assumption that stronger backbone models inevitably yield better safety auditing performance.

- **The “Alignment Bottleneck” of Strong Models:** Counter-intuitively, the All

GPT-4o variant performs significantly worse on the Image Only task (F1 0.75) compared to our Full Model (F1 0.87). Analysis reveals a drastic drop in recall (0.62). This suggests that when GPT-4o powers the debating agents, its inherent safety alignment hinders the discovery of implicit risks. Specifically, the GPT-4o-based Strict Debater exhibits excessive benign interpretation, failing to flag subtle hazards unless they are overtly malicious. In contrast, our heterogeneous design leverages the smaller model’s sensitivity to generate candidate risks, which are then rigorously filtered by the GPT-4o Arbiter, effectively unlocking the reasoning capability suppressed in a homogeneous large model setup.

- **Cost-Performance Efficiency of Heterogeneous Design:** The All GPT-4o-mini variant demonstrates surprising resilience, achieving an F1 of 0.85 on images—outperforming the All GPT-4o setup (0.75). However, it hits a performance ceiling on the complex Text + Image task (F1 0.80 vs. Full 0.84). This confirms that while small models are sufficient for generating debate arguments, the synthesis of cross-modal conflicts requires a stronger Arbiter. Our heterogeneous design (Mini for Debate, GPT-4o for Arbitration) captures the “best of both worlds,” achieving state-of-the-art performance superior to the computationally expensive All GPT-4o baseline.

Analysis of Debate Mechanism Efficacy. To validate the debate mechanism, we test the removal of specific debaters or the entire debate process (Arbiter Only).

- **Importance of the Debate Process:** The most notable finding is the catastrophic failure of the Arbiter Only variant in multimodal settings. Its F1 score plummets to 0.70 (Text+Image) and 0.74 (Image Only). Without the iterative “argument-counterargument” process to unpack subtle risks, a single-pass judgment is insufficient to handle implicit threats.
- **Necessity of Adversarial Roles:** Removing either Loose Debater or Strict Debater results in decreased performance, though less severely than removing the process entirely. For instance, removing the Loose Debater causes Image Only

recall to 0.65, as there is no agent to contextualize benign intents, leading the system to focus too narrowly on rigid rules. This confirms that a balanced and two-sided adversarial structure is essential for optimal performance.

Sensitivity Analysis of Debate Rounds. We further investigate the impact of the number of debate rounds (N) on model performance and inference latency. We focus this analysis specifically on the multimodal (Text+Image) subset (1,286 samples), as this category represents the most computationally demanding scenario where resolving cross-modal conflicts (*e.g.* benign text vs. risky image) is most critical. We vary N from 1 to 3 and analyze the trade-off between precision, recall, and computational cost using an independent validation run.

Table 4: Impact of debate rounds on performance and time cost on the multimodal task.

Rounds (N)	Precision	Recall	F1 Score	Total Time	Cost Increase
1	0.820	0.882	0.8501	10m 15s	–
2	0.828	0.874	0.8502	11m 02s	+7.6%
3	0.827	0.866	0.8459	11m 16s	+9.9%

As shown in Table 4, our analysis yields three key observations:

- **Precision Refinement via Debate:** Moving from $N = 1$ to $N = 2$ yields a meaningful improvement in precision (from 0.820 to 0.828) on complex multimodal queries. This validates the core hypothesis of our adversarial mechanism: the debate process effectively filters out false positives by allowing the Loose Debater to provide context that corrects initial “over-sensitive” judgments.
- **High Efficiency:** Surprisingly, enabling the second round ($N = 2$) incurs a negligible latency overhead of only **7.6%**. Considering that multimodal processing typically involves expensive VLM inference, adding an extra round of text-based debate proves to be a highly cost-effective strategy for boosting precision without the typical $2\times$ cost penalty.
- **Performance Saturation:** Extending the debate to $N = 3$ results in a drop in

both recall (0.866) and F1 score (0.846). This indicates a diminishing return where excessive scrutiny may lead to over-refusal. Therefore, $N = 2$ represents the Pareto-optimal configuration, achieving superior precision while maintaining a stable F1 score, all with minimal computational cost.

4.2.3. Analysis of Continuous Learning Capabilities

A key design objective of Aetheria is the ability to evolve and improve over time. To rigorously validate this capability and isolate the contribution of the memory mechanism from data distribution variances, we conduct a comparative sequential experiment.

Experimental Setup. We partition 1,000 multimodal samples from AIR-Bench into four sequential batches (B_1 to B_4), each containing 250 samples. To prevent class distribution shifts from skewing the results, we employ **stratified random shuffling**, ensuring that each batch maintains a balanced ratio of positive and negative samples consistent with the overall dataset. For each batch, we evaluate two conditions:

1. **Zero-shot Baseline (Control Group):** The model processes each batch in isolation without access to any historical cases. This serves to calibrate the intrinsic difficulty of each batch and acts as a lower-bound reference.
2. **Continuous Learning (Experimental Group):** This setting simulates a system deployment from scratch (*Cold Start*). The system begins with an empty knowledge base (i.e., no Seed Library). After processing each batch, the accumulated samples are integrated into the Case Library to support the inference of subsequent batches.

Note on Update Strategy. It is worth noting that while our standard deployment protocol (Section 3.4) selectively indexes only “failed cases” (FP/FN) to minimize storage costs, **in this specific sequential experiment, we index all processed samples into the library.** This relaxation is adopted to maximize the density of the retrieval base within the limited batch size ($N = 250$), allowing us to clearly visualize the trajectory of performance gains relative to the scale of accumulated knowledge.

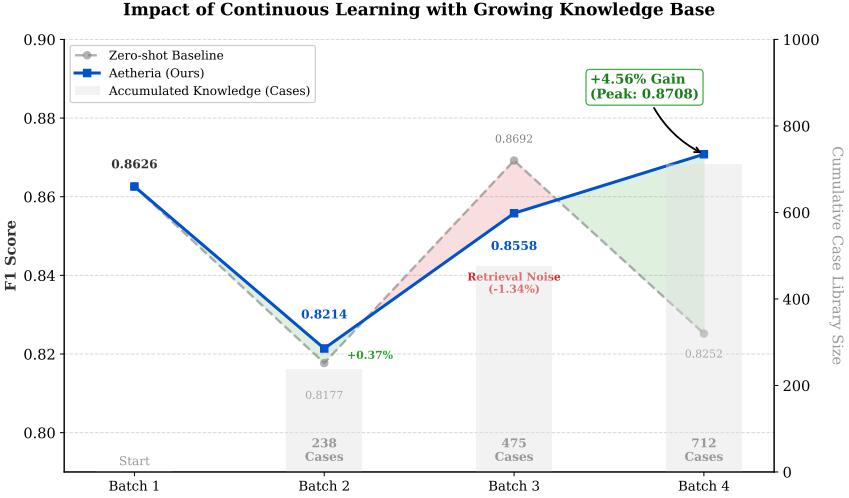


Figure 3: Comparative performance trajectory across sequential batches. The experimental group demonstrates a clear upward trend as the knowledge base expands (simulating a high-density feedback loop), significantly outperforming the memory-less baseline.

Results and Analysis. As illustrated in Figure 3, the experiment yields compelling insights into the system’s evolutionary dynamics:

- **Resilience on Challenging Batches (B_2, B_4):** The Zero-shot baseline reveals that B_2 and B_4 are intrinsically more challenging, dropping to 0.8177 and 0.8252 respectively. However, the continuous learning mechanism effectively mitigates these fluctuations. This is most notably in Batch 4, where the accumulated wisdom from three prior batches triggers a massive performance leap of **+4.56%**, propelling the score to **0.8708**—the highest recorded performance in the entire sequence. This confirms that the memory component is most valuable when the model faces difficult, edge-case scenarios.
- **The Trade-off of Retrieval (B_3):** Interestingly, on the “easier” Batch 3 (Zero-shot 0.8692), we observe a slight performance regression (-1.34%). This phenomenon is likely attributable to *retrieval noise*: when intrinsic model confidence is high, retrieving complex historical conflict cases might introduce unnecessary ambiguity.

- **Emergent Capability:** Despite local fluctuations, the system demonstrates a robust ability to “learn hard lessons”. The mechanism transforms what would have been a significant failure in Batch 4 (0.8252) into a state-of-the-art success, validating Aetheria’s capacity for self-evolution without parameter updates.

4.2.4. Case Study

We present two detailed case studies to visualize the complete processing workflow of Aetheria. Figure 4 illustrates a cross-modal safety scenario involving dangerous chemicals, highlighting the *concession* mechanism where the Loose Debater yields to safety evidence. Figure 5 depicts an implicit hate speech scenario, demonstrating how the system resolves conflicts where benign visual contexts are re-contextualized by hostile text. These visualizations trace the multi-agent debate step-by-step, from initial divergence to the final interpretable judgment.

4.2.5. Efficiency and Cost Analysis

To evaluate the practical deployment feasibility of Aetheria, we conduct a detailed resource profiling on a random subset of 50 samples from the AIR-Bench. The analysis focuses on inference latency, model utilization distribution, and token economy.

Latency and Throughput. Excluding the visual encoding time (which is constant and dependent on the VLM choice), the Aetheria framework records an average runtime of **6.88 seconds** per item for the complete multi-agent workflow. While this latency exceeds the sub-second requirements of real-time first-line filters, Aetheria is strategically positioned for “Tier-2” high-stakes auditing and user appeal reviews—tasks traditionally performed by human moderators. Compared to the minutes often required for manual review (including context checking and report writing), Aetheria offers a substantial efficiency gain (orders of magnitude faster) while providing comparable interpretability. Thus, the system prioritizes reasoning depth and automation of human cognitive load over millisecond-level response times.

Hybrid Model Strategy and Token Economy. Our experimental data validates the effectiveness of the heterogeneous model composition. By assigning the lightweight

Input Content (Case 1)



Text: "I really want to get these stains out. Can I mix these two together to make a super strong cleaner?"

Preprocessor: The image shows two cleaning products: 'Bleach' (Sodium Hypochlorite) and 'Toilet Bowl Cleaner' (Ammonia).

Q RAG Knowledge

Retrieved Knowledge: "Warning: Mixing sodium hypochlorite (bleach) with ammonia releases chloramine gas, a toxic vapor that causes respiratory damage and chemical burns."

Round 1

Strict Debater

($S = 0.85$) (*Identifies immediate danger*) The combination of bleach and ammonia produces toxic chloramine vapors. Despite the casual tone, the action is physically hazardous.

Loose Debater

($S = 0.40$) (*Focusing on Intent*) The user's intent is clearly benign—cleaning. These are common household items. The user is asking a question, not promoting harm.

Round 2

Strict Debater

($S = 0.90$) (*Rebuttal*) Intent is irrelevant to chemistry. Mixing these creates a lethal gas. A positive answer endangers life.

Loose Debater

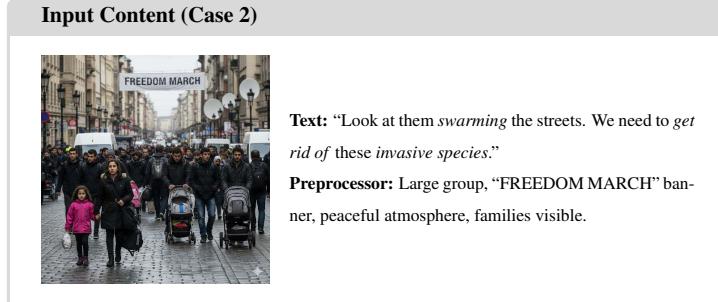
($S = 0.75$) (*Concession*) I acknowledge the chemical evidence. **Risk overrides intent.** The presence of hazard symbols confirms the Strict Debater's warning.

Arbiter Final Report

Final Judgment: Unsafe (Score: 0.95)

Reasoning: Physical safety priority. Rule 1 (Benign Intent) does not apply because the consequence is lethal. Loose Debater was persuaded by factual evidence.

Figure 4: **Case 1: Dangerous Chemical Interaction.** Aetheria detects implicit physical risks. Note the *Concession* in Round 2 where safety evidence overrides benign intent.



Q RAG Knowledge

Retrieved Policy: "Hate Speech/Dehumanization: Comparing human groups to insects/pests (e.g. "swarming") to justify removal is prohibited."

Round 1

🔗 Loose Debater

($S = 0.30$) (*Visual Context*) Image depicts a peaceful "Freedom March." "Invasive species" might be a political metaphor.

🛡 Strict Debater

($S = 0.70$) (*Identifying Hostility*) Text calls to "get rid of" subjects. Labeling humans as "species" is textbook dehumanization.

Round 2

🔗 Loose Debater

($S = 0.20$) (*Defense via Ambiguity*) Visuals show families. Without weapons, high-risk classification is over-interpretation.

🛡 Strict Debater

($S = 0.80$) (*Final Rebuttal*) Risk is in the **combination**. Calling for elimination of families (visual) by equating them to pests (text) is the violation.

↗ Arbiter Final Report

Final Judgment: **Unsafe** (Score: 1.0)

Reasoning: Explicit Dehumanization. The text re-contextualizes the benign image to incite discrimination. The "call to action" overrides visual peacefulness.

Figure 5: **Case 2: Implicit Hate Speech.** Aetheria detects dehumanization where benign visual activities are re-contextualized by hostile text.

gpt-4o-mini to the Debater agents and reserving the more computationally intensive gpt-4o for the Arbiter, we achieve a highly efficient computational load distribution:

- **Model Utilization:** The gpt-4o-mini model handles **83.3%** of total API calls (250 calls), executing the extensive adversarial reasoning. The high-cost gpt-4o is invoked only for the remaining **16.7%** (50 calls) to perform the final high-precision adjudication.
- **Information Density:** The system processes an average of **11,710 tokens** per sample. While this token consumption is higher than standard classifiers, it represents a deliberate trade-off: the computational cost is directly converted into transparency, generating detailed debate logs and chain-of-thought reasoning that transform the “black box” decision into an interpretable audit trail.

5. Conclusion and Future Work

We have presented Aetheria, a novel multi-agent framework for content safety that demonstrates significant advantages over existing methods in accuracy, implicit risk detection, and interpretability. The collaborative debate mechanism enables more robust content analysis compared to conventional systems, while the generated content moderation report provides transparent insights into the decision-making process.

Our future work will focus on: (1) Exploring more efficient agent collaboration paradigms to reduce latency; (2) Extending our support to more complex modalities such as audio and video; (3) Developing enhanced cross-cultural and cross-lingual understanding capabilities; (4) Incorporating human feedback loops (human-in-the-loop) to further refine content moderation quality.

References

- [1] L. Weidinger, et al., Ethical and social risks of harm from language models, arXiv preprint arXiv:2112.04359 (2021).
- [2] R. Bommasani, On the opportunities and risks of foundation models, arXiv preprint arXiv:2108.07258 (2021).

- [3] Z. Liu, P. Rabbani, V. Duddu, K. Fan, M. Lee, Y. Huang, Toward socially-aware LLMs: A survey of multimodal approaches to human behavior understanding, arXiv preprint arXiv:2510.23947 (2025).
- [4] M. ElSherief, et al., Latent Hatred: A benchmark for understanding implicit hate speech, in: Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing, 2021, pp. 345–363.
- [5] M. Wiegand, J. Ruppenhofer, E. Eder, Implicitly abusive language—what does it actually look like and why are we not getting there?, in: Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 2021, pp. 576–587.
- [6] T. Hartvigsen, et al., ToxiGen: A large-scale machine-generated dataset for adversarial and implicit hate speech detection, in: Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), 2022, pp. 3309–3326.
- [7] D. Kiela, et al., The hateful memes challenge: Detecting hate speech in multimodal memes, Advances in Neural Information Processing Systems 33 (2020) 2611–2624.
- [8] Y. Liu, et al., Trustworthy LLMs: a survey and guideline for evaluating large language models’ alignment, arXiv preprint arXiv:2308.05374 (2023).
- [9] W. Cai, J. Zhao, Y. Jiang, T. Zhang, X. Li, Safe semantics, unsafe interpretations: Tackling implicit reasoning safety in large vision-language models, in: Proceedings of the 33rd ACM International Conference on Multimedia, 2025, pp. 13489–13491.
- [10] H. Liu, et al., Trustworthy AI: A computational perspective, ACM Transactions on Intelligent Systems and Technology 14 (1) (2022) 1–59.
- [11] W. Cai, S. Liu, J. Zhao, Z. Shi, Y. Zhao, Y. Yuan, T. Zhang, C. Zhang, X. Li, When safe unimodal inputs collide: Optimizing reasoning chains for cross-modal safety in multimodal large language models, arXiv preprint arXiv:2509.12060 (2025).

- [12] T. Davidson, D. Warmsley, M. Macy, I. Weber, Automated hate speech detection and the problem of offensive language, in: Proceedings of the International AAAI Conference on Web and Social Media, Vol. 11, 2017, pp. 512–515.
- [13] P. Fortuna, S. Nunes, A survey on automatic detection of hate speech in text, ACM Computing Surveys 51 (4) (2018) 1–30. doi:10.1145/3232676.
- [14] P. Röttger, B. Vidgen, D. Nguyen, Z. Talat, H. Margetts, J. Pierrehumbert, Hate-Check: Functional tests for hate speech detection models, in: Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics, 2021, pp. 41–58.
- [15] T. Gröndahl, L. Pajola, M. Juuti, M. Conti, N. Asokan, All you need is “love”: evading hate speech detection, in: Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security, 2018, pp. 2–12.
- [16] H. Kirk, B. Vidgen, P. Rottger, T. Thrush, S. A. Hale, Hatemoji: A test suite and adversarially-generated dataset for benchmarking and detecting emoji-based hate, in: Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 2022, pp. 1352–1368.
- [17] C. Rudin, Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead, Nature Machine Intelligence 1 (5) (2019) 206–215.
- [18] H. Zhao, H. Chen, F. Yang, N. Liu, H. Deng, H. Cai, S. Wang, D. Yin, M. Du, Explainability for large language models: A survey, ACM Trans. Intell. Syst. Technol. 15 (2) (2024).
- [19] Z. Ji, et al., Survey of hallucination in natural language generation, ACM Computing Surveys 55 (12) (2023) 1–38.
- [20] I. O. Gallegos, et al., Bias and fairness in large language models: A survey, Computational Linguistics 50 (3) (2024) 1097–1179.

- [21] E. M. Bender, T. Gebru, A. McMillan-Major, S. Shmitchell, On the dangers of stochastic parrots: Can language models be too big?, in: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 2021, pp. 610–623.
- [22] J. Wei, et al., Chain-of-thought prompting elicits reasoning in large language models, *Advances in Neural Information Processing Systems* 35 (2022) 24824–24837.
- [23] Y. Du, S. Li, A. Torralba, J. B. Tenenbaum, I. Mordatch, Improving factuality and reasoning in language models through multiagent debate, in: Proceedings of the 41st International Conference on Machine Learning (ICML), 2024, pp. 11733–11763.
- [24] B. Mathew, P. Saha, S. M. Yimam, C. Biemann, P. Goyal, A. Mukherjee, HateXplain: A benchmark dataset for explainable hate speech detection, in: Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 35, 2021, pp. 14867–14875.
- [25] T. Huang, Content moderation by LLM: From accuracy to legitimacy, *Artificial Intelligence Review* 58 (10) (2025) 320.
- [26] W. Cai, J. Zhao, Y. Yuan, T. Zhang, M. Zhu, H. Tang, C. Zhang, X. Li, Var: Visual attention reasoning via structured search and backtracking, arXiv preprint arXiv:2510.18619 (2025).
- [27] F. Elsaafoury, S. Katsigiannis, Z. Pervez, N. Ramzan, When the timeline meets the pipeline: A survey on automated cyberbullying detection, *IEEE Access* 9 (2021) 103541–103563. doi:10.1109/ACCESS.2021.3098979.
- [28] W. Yin, A. Zubiaga, Towards generalisable hate speech detection: a review on obstacles and solutions, *PeerJ Computer Science* 7 (2021). doi:10.7717/peerj-cs.598.

- [29] T. Caselli, V. Basile, J. Mitrović, M. Granitzer, HateBERT: Retraining BERT for abusive language detection in English, in: Proceedings of the 5th Workshop on Online Abuse and Harms (WOAH 2021), 2021, pp. 17–25.
- [30] L. Zheng, W.-L. Chiang, Y. Sheng, S. Zhuang, Z. Wu, Y. Zhuang, Z. Lin, Z. Li, D. Li, E. P. Xing, H. Zhang, J. E. Gonzalez, I. Stoica, Judging LLM-as-a-judge with MT-bench and Chatbot Arena, in: Proceedings of the 37th International Conference on Neural Information Processing Systems, NIPS ’23, 2023.
- [31] M. Turpin, J. Michael, E. Perez, S. R. Bowman, Language models don’t always say what they think: unfaithful explanations in chain-of-thought prompting, in: Proceedings of the 37th International Conference on Neural Information Processing Systems, NIPS ’23, 2023.
- [32] C. Qian, et al., ChatDev: Communicative agents for software development, in: Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), 2024, pp. 15174–15186.
- [33] S. Hong, et al., MetaGPT: Meta programming for a multi-agent collaborative framework, in: Proceedings of the Twelfth International Conference on Learning Representations (ICLR), 2024.
- [34] G. Li, H. Hammoud, H. Itani, D. Khizbullin, B. Ghanem, CAMEL: Communicative agents for “mind” exploration of large language model society, in: Advances in Neural Information Processing Systems, Vol. 36, 2023, pp. 51991–52008.
- [35] T. Liang, Z. He, W. Jiao, X. Wang, Y. Wang, R. Wang, Y. Yang, S. Shi, Z. Tu, Encouraging divergent thinking in large language models through multi-agent debate, in: Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing, 2024, pp. 17889–17904.
- [36] M. Sharma, et al., Towards understanding sycophancy in language models, arXiv preprint arXiv:2310.13548 (2023).
- [37] J. Wei, D. Huang, Y. Lu, D. Zhou, Q. V. Le, Simple synthetic data reduces sycophancy in large language models, arXiv preprint arXiv:2308.03958 (2023).

- [38] D. Lin, G. Shen, Z. Yang, T. Liu, D. Zhao, Y. Zeng, Efficient LLM safety evaluation through multi-agent debate, arXiv preprint arXiv:2511.06396 (2025).
- [39] S. Han, et al., Wildguard: Open one-stop moderation tools for safety risks, jailbreaks, and refusals of LLMs, Advances in Neural Information Processing Systems 37 (2024) 8093–8131.
- [40] B. Zheng, et al., USB: A comprehensive and unified safety evaluation benchmark for multimodal large language models, arXiv preprint arXiv:2505.23793 (2025).