

# A Survey on Collaborating Small and Large Language Models for Performance, Cost-effectiveness, Cloud-edge Privacy, and Trustworthiness

Fali Wang, Jihai Chen\*, Shuhua Yang, Ali Al-Lawati, Linli Tang

Pennsylvania State University  
University Park, USA

Hui Liu  
Michigan State University  
East Lansing, USA

Suhang Wang<sup>†</sup>  
Pennsylvania State University  
University Park, USA

## Abstract

Large language models (LLMs) have achieved remarkable progress across domains and applications, but face challenges such as high fine-tuning costs, inference latency, limited edge deployability, and reliability concerns. Small language models (SLMs), with compact, efficient, and adaptable features, offer promising solutions. Building on this potential, recent research explores collaborative frameworks that integrate their complementary strengths, leveraging SLMs' specialization and efficiency with LLMs' generalization and reasoning, to address diverse objectives across tasks and deployment scenarios. Motivated by these developments, this paper presents a systematic survey of SLM-LLM collaboration from the perspective of collaboration objectives. We propose a taxonomy covering four goals: *performance enhancement*, *cost-effectiveness*, *cloud-edge privacy*, and *trustworthiness*. Under this framework, we review representative methods, summarize design paradigms, and outline open challenges and future directions toward efficient and secure SLM-LLM collaboration. The collected papers are available in [link here](#).

## 1 Introduction

Large language models (LLMs) have profoundly transformed multiple domains, including AI for science (Luo et al., 2022; Al-Lawati et al., 2025; Wang et al., 2024a,d), programming (Shi et al., 2024), and human-centered interaction (Zhang et al., 2024c), primarily owing to their massive parameter scales. However, such scale also introduces several challenges: (1) fine-tuning is computationally intensive, limiting efficient model adaptation (Thawakar et al., 2025; Liu et al., 2024d; Xia et al., 2024; Zhang et al., 2024h); (2) large model size leads to inference latency, constraining real-time applications (Leviathan et al., 2023;



Figure 1: Detailed taxonomy of SLM-LLM collaboration, depicting the sub-taxonomy under the collaboration objectives of *performance*, *cost-effectiveness*, *privacy*, and *trustworthiness*.

Kwon et al., 2023; Cai et al., 2024); (3) typical edge devices, such as mobile phones, personal computers, and small servers, lack the capacity to host these models, while cloud-based inference raises privacy and cost concerns (Carlini et al., 2021; Xu et al., 2024c; Li et al., 2024b); and (4) LLMs exhibit inherent reliability risks, including hallucinations and jailbreak vulnerabilities (Yao et al., 2024; Farquhar et al., 2024; Wang et al., 2023a). These challenges underscore the increasing need for customizable, cost-efficient, edge-deployable, and trustworthy AI solutions. Small language models (SLMs), characterized by their compact architecture, low computational cost, and adaptability, have emerged as promising counterparts to mitigate these issues, although their general reasoning and knowledge coverage remain more limited than those of LLMs. Consequently, harnessing the complementary strengths of SLMs and LLMs provides a viable pathway toward developing efficient, scalable, and reliable intelligent systems.

Researchers have developed various approaches to enable collaboration between SLMs and LLMs, leveraging the strengths of SLMs in customization, efficiency, and local deployment, alongside

\* Work done as an intern at Penn State.

<sup>†</sup> Corresponding author. Email: szw494@psu.edu

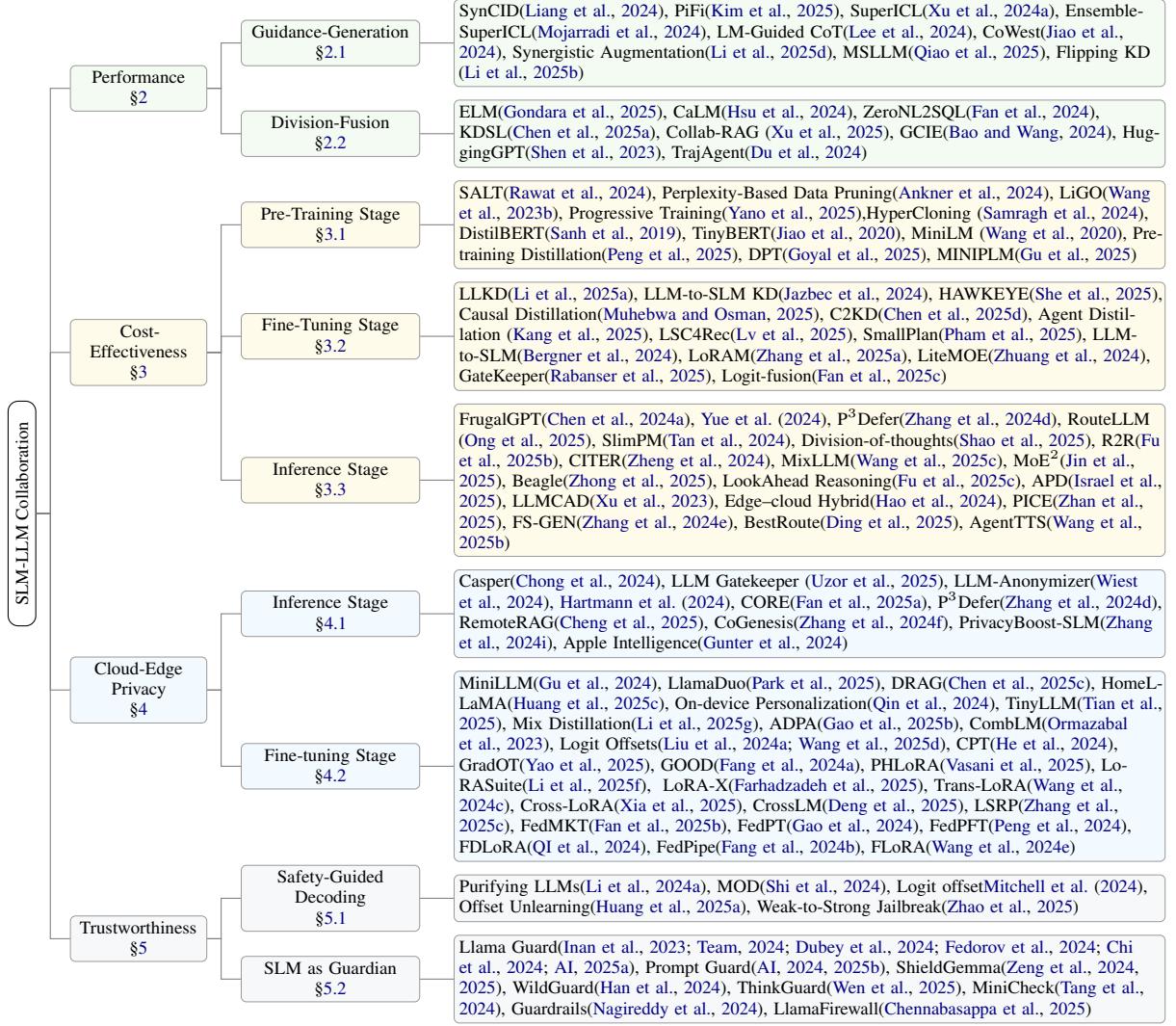


Figure 2: A Taxonomy of SLM-LLM Collaboration.

the powerful generalization capabilities of LLMs (Xu et al., 2024a; Chen et al., 2024a; Wang et al., 2025b; Gu et al., 2024; Inan et al., 2023). Despite the importance of this topic and the various approaches developed, there is a lack of a systematic survey centered on the **objectives of SLM-LLM collaboration**. Hence, we fill this gap by providing a taxonomy that unifies recent works under clear collaboration objectives. Existing studies generally pursue four main objectives. First, by combining domain-specific SLMs that outperform general-purpose LLMs in specialized contexts, many works target collaboration for enhanced *task performance* across both general and domain-specific tasks. Second, emphasizing *cost-effectiveness*, SLMs are employed for lightweight processing, while LLMs are invoked selectively when necessary. Third, under the paradigm of *cloud-edge collaboration*, on-device SLMs pro-

cess privacy-sensitive data, whereas cloud-based LLMs provide general reasoning, ensuring both effectiveness and privacy. Finally, SLMs act as lightweight *safety policy encoders*, while LLMs serve as backbone generators to improve output *trustworthiness*. Therefore, our survey is organized around the objectives of SLM-LLM collaboration: *performance*, *cost-effectiveness*, *cloud-edge privacy*, and *trustworthiness*. Under this framework, we propose a taxonomy of existing studies (in Fig. 2 and Tab. 1), summarize key insights, and outline future directions for efficient, secure, and deployable intelligent systems.

**Differences from existing surveys** Several surveys have examined SLMs in the LLM era. Wang et al. (2024b, 2025a) provided a broad overview of SLM design, acquisition, applications, and trustworthiness but mentioned SLM-LLM collaboration only briefly. Lu et al. (2024) evaluated

SLM advantages through experimental analysis, Van Nguyen et al. (2024) focused on architectures and compression techniques, and Xu et al. (2024c) discussed on-device deployment, all with limited discussion of collaboration. Existing collaboration surveys also remain narrow: Chen and Varoquaux (2024) explored one-way collaboration (SLMs for LLMs or LLMs for SLMs), whereas Niu et al. (2025); Li et al. (2025c) examined cloud–edge collaboration without addressing diverse collaboration objectives. To fill this gap, we systematically review existing studies from the perspective of collaboration objectives, summarizing key insights to guide future SLM–LLM collaboration.

Our main contributions are summarized as follows: (1) We present the first systematic survey of SLM–LLM collaboration from a novel perspective centered on collaboration objectives, encompassing performance, cost-effectiveness, cloud–edge privacy, and trustworthiness. The overall taxonomy is illustrated in Fig. 2. (2) We analyze and categorize performance-oriented collaboration studies based on how they exploit the complementary strengths of SLMs and LLMs, forming two major paradigms: Guidance–Generation and Division–Fusion. (3) We summarize cost-effectiveness-driven collaboration along the lifecycle of language models, covering the pre-training, fine-tuning, and inference stages. (4) We review privacy-preserving collaboration between cloud and edge models according to how edge data are privately leveraged by cloud models during both the inference and fine-tuning stages. (5) We discuss trustworthiness-oriented collaboration under two paradigms: safety-guided decoding and guardian–generator frameworks.

## 2 Collaboration for Performance

The optimal LLM varies across tasks and queries (Jiang et al., 2023; Ashiga et al., 2025; Bell, 2025; Wang et al., 2025b), making single-model solutions suboptimal. Leveraging complementary models is therefore effective. Owing to their customizability, SLMs have produced many domain-specific products, such as SciGLM (Zhang et al., 2024a), Chem-LLM (Zhang et al., 2024b), and Biomstral (Labrak et al., 2024). Hence, SLM–LLM collaboration for performance has been a prevalent strategy. We divide existing works mainly into two paradigms: (1) *Guidance–Generation*, where one model steers another’s generation, and (2) *Division–Fusion*, where the SLMs and LLMs leverage their complementary

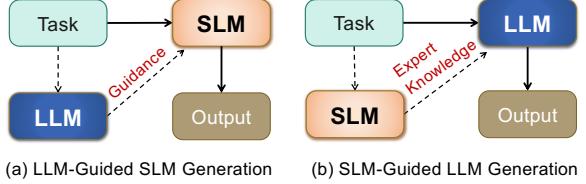


Figure 3: Guidance-Generation Collaboration.

strengths on distinct tasks.

### 2.1 Guidance–Generation Collaboration

Guidance–Generation collaboration involves one assistant model providing guidance based on its strengths to support a backbone model in generation. When one model performs well overall and another excels in a specific aspect, the former serves as the generator while the latter offers complementary guidance. This paradigm generally appears in two forms: (1) LLM-guided SLM generation and (2) SLM-guided LLM generation.

**(1) LLM-guided SLM generation.** As shown in Fig. 3(a), the LLM uses its semantic understanding to provide fine-grained guidance for task-specific SLMs. For example, SyncID (Liang et al., 2024) employs LLM-generated task descriptions to guide SLM reasoning. PiFi (Kim et al., 2025) uses LLMs’ certain knowledge layer plug-in to enhance SLM’s generalization and understanding.

**(2) SLM-guided LLM generation.** As shown in Fig. 3(b), the SLM offers domain expertise and cues, while the LLM integrates this information for more accurate and reliable outputs. For instance, SuperICL and its variant (Xu et al., 2024a; Mojarradi et al., 2024) inject SLM predictions and confidence scores into the LLM’s context, and LM-Guided CoT (Lee et al., 2024) uses SLM-generated reasoning chains to guide LLM inference. CoWest (Jiao et al., 2024) aligns weak–strong preferences to synergize domain expert SLMs’ knowledge and LLMs’ general reasoning. Synergistic Augmentation (Li et al., 2025d) uses SLM to guide LLM with confident demonstrations and slot hints, boosting zero-shot slot filling performance. MSLLM (Qiao et al., 2025) combines SLM’s precise error detection with LLM’s fluency and semantic understanding for superior Chinese spelling correction. Flipping KD (Li et al., 2025b) enables LLMs to learn task-specific ability from SLMs.

Table 1: Representative works on collaborations across performance, cost-effectiveness, privacy, and trustworthiness.

Collab. Mechanism	Paper	SLM	LLM	Evaluation Dataset	Goal / Contribution
<b>I. Collaboration for Performance</b>					
<b>LLM guided SLM</b>	SynCID (2024)	BERT	GPT-3.5	Banking77, CLINC150	Refine labels for intent detection
<b>LLM guided SLM</b>	PiFi (2025)	BERT, T5	LLaMA 3.1-8B	SST-2, IMDB, etc.	Frozen LLM layer enhances SLM
<b>SLM guided LLM</b>	SuperICL (2024a)	RoBERTa	GPT-3.5/4	SST-2, MNLI, etc.	Inject SLM predictions and confidence
<b>SLM guided LLM</b>	Ensem. SuperICL (2024)	BERT/RoBERTa	GPT-3.5/LLaMA	SST-2, MNLI, etc.	Multi-SLM guidance for LLMs
<b>SLM guided LLM</b>	LM-Guided CogT (2024)	Flan-T5	ChatGPT	HotpotQA, 2WikiMultiHopQA	Provide rationales to improve reasoning
<b>SLM guided LLM</b>	CoWest (Jiao et al., 2024)	LLaMA-3-8B	GPT-4/3.5	IfQA, MedMCQA, etc.	Preference-aligned weak-to-strong collab.
<b>Parallel</b>	ELM (2025)	ClinicalBERT	GPT-4	BCCR Pathology Reports	Aggregate SLM votes; LLM verifies
<b>Parallel</b>	CaLM (2024)	T5, Flan-T5	Flan-PaLM, GPT-3.5	QAGS-CNNMD, Q <sup>2</sup> , etc.	Cross-verification SLM ↔ LLM
<b>Sequential</b>	ZeroNL2SQL (2024)	T5, BART	GPT-3.5/4	Spider, WikiSQL, etc.	SLM drafts SQL; LLM finalizes
<b>Sequential</b>	KDSL (2025a)	Qwen2-VL 2B	Qwen2-VL 7B	—	SLM rules; LLM inference
<b>Sequential</b>	HuggingGPT (2023)	CLIP, BLIP, T5	GPT-3.5	ImageNet, COCO, etc.	LLM orchestrates multimodal SLMs
<b>II. Collaboration for Cost-effectiveness</b>					
<b>Data curation</b>	SALT (2024)	Transformer-1.5B	Transformer-2.8B	Pile	SLM-guided data selection
<b>Data curation</b>	Ankner et al. (2024)	MPT-125M	MPT-1B/3B	The Pile, Dolma, etc.	SLM perplexity-guided efficient pruning
<b>Co-curriculum</b>	Yano et al. (2025)	LLaMA-1B	LLaMA-8B	FineWeb-Ed	Joint curriculum design
<b>Co-curriculum</b>	LiGO (2023b)	BERT-S, DeiT-S	BERT-B, DeiT-B	GLUE, SQuAD, ImageNet	Learned growth reduces training cost
<b>Co-curriculum</b>	HYPERCLONING (2024)	OPT-350M	OPT-1.3B	DOLMA, The Pile, etc.	Function-preserving SLM-to-LLM initial.
<b>Pre-train distill.</b>	Peng et al. (2025)	GLM-4.1.9B	GLM-4.9B	MMLU, C-Eval, etc.	Progressive knowledge transfer
<b>Pre-train distill.</b>	DPT (2025)	—	—	Synthetic bigram data	Distillation improves scaling, harms ICL
<b>Pre-train distill.</b>	MINIPLM (2025)	Qwen 200M/500M	Qwen 1.5-1.8B	DCLM subset	Offline sampling accelerates pretraining
<b>Selective KD</b>	SynCID (2024)	BERT	text-davinci-003	BANKING, CLINC	Latent-space alignment distillation
<b>Selective KD</b>	LLM-to-SLM (2024)	T5-Small	T5-Large	WMT, CNN, etc.	Frozen LLM conditions fast SLM
<b>Proxy transfer</b>	LiteMoE (2024)	Gemma-2B	Gemma-7B	MMLU, GSM8K, etc.	Efficient proxy tuning
<b>Proxy transfer</b>	GateKeeper (2025)	Gemma-2B	Gemma-7B	CIFAR, ARC, VQA2, etc.	Conf-tuned SLM improves cascading
<b>Proxy transfer</b>	G-Boost (2025c)	TinyLlama-1B	LLaMA2-13B	GSM8K, MATH-500	Reward-guided dynamic collaboration
<b>Cascade Routing</b>	R2R (2025b)	DeepSeek-R1-1.5B	DeepSeek-R1-32B	AIME, GPQA	Token-level routing for efficiency
<b>Cascade Routing</b>	SlimPM (2024)	LLaMA2-7B	LLaMA2-70B	NQ, TriviaQA, etc.	Proxy-guided selective retrieval efficiency
<b>Cascade Routing</b>	CITER (2024)	Qwen2-1.5B	Qwen2-72B	CSQA, ARC, etc.	Token-level routing boosts efficiency
<b>Cascade Routing</b>	MixLLM (2025c)	Llama-3-8B	GPT-3.5/4, etc.	RouterBench	Adaptive routing
<b>Speculative</b>	Beagle (2025)	LLaMA-68M	LLaMA-7B	ShareGPT	Cross-attention drafting
<b>Speculative</b>	APD (2025)	Qwen2.5-0.5B	Dream-7B	GSM8K, GPQA, MATH	Adaptive parallel decoding via PoE
<b>Speculative</b>	LLMCAD (2023)	GPT-2/lnT5	Vicuna/LLaMA2	CNN/DailyMail, etc.	Token-tree drafting
<b>Speculative</b>	Cloud-edge (2024)	TinyLlama	GPT-3.5	GSM8K	Token-level edge-cloud collaboration
<b>Optimal TTS</b>	AgentTTS (2025b)	LLaMA-3-3B	LLaMA-3-70B	HotpotQA, CWQ, etc.	Budget-aware collaboration
<b>Optimal TTS</b>	BestRoute (2025)	Phi-3-mini/medium, etc.	GPT-4/3.5	MixInstruct, RewardBench, etc.	Adaptive routing minimizes cost
<b>III. Privacy-aware Cloud–Edge Collaboration</b>					
<b>PII Gatekeeper</b>	Uzor et al. (2025)	Phi-3.5, Gemma-2	GPT-4o	HealthTap, MeQSum	Rewrite prompts to remove PII
<b>PII Gatekeeper</b>	LLM-Anonymizer (2024)	Llama-3 8B, etc.	Any	real clinical letters	Local LLM anonymization
<b>PII Gatekeeper</b>	P <sup>3</sup> Defer (2024d)	Gemma-2B	Gemma-7B	GSM8K, MedSum, etc.	CoT policy RL reduces leakage
<b>All-info Guardian</b>	CoGenesis (2024f)	StableLM-Zephyr	GPT-4-turbo	Avocado Research Email	Cloud knowledge for edge inference
<b>All-info Guardian</b>	Hartmann et al. (2024)	Gemini 1.0 Nano-2	Gemini 1.0 Ultra	GSM8K	Cloud ICL demos for edge SLM
<b>All-info Guardian</b>	PrivacyBoost-SLM (2024i)	BioLinkBERT, etc.	GPT-3.5	MedQA, HEADQA, etc.	Privacy prompting boosts medical QA
<b>SLM as Learner</b>	MiniLLM (2024)	GPT-2-125M	GPT-2-1.5B	DollyEval, SelfInst, etc.	Distill LLM into SLM
<b>SLM as Learner</b>	Mix Distillation (2025g)	Qwen2.5-0.5B, etc.	QwQ-32B, etc.	MATH, GSM8K, etc.	Learnability gap, mixed distillation
<b>LLM as Learner</b>	Proxy-tuning (2024a)	LLaMA-2-7B	LLaMA-2-70B	GSM, Toxigen, etc.	Steer LLM with private SLM
<b>LLM as Learner</b>	CrossLoRA (2025)	Qwen2.5-1.5B/3B, etc.	Hetero-families	ARC-c, ARC-e, OBQA, etc.	Zero-data subspace LoRA transfer
<b>Co-learners</b>	FDLora (2024)	LLaMA-2-7B	LLaMA-2-7B	BGL, Spirit, etc.	Federated LoRA with sharing
<b>Co-learners</b>	FedMKT (2025b)	GPT-2-xl, OPT, etc.	LLaMA2-7B	RTE, WIC, BoolQ, etc.	Bidirectional federated co-distillation
<b>IV. Collaboration for Trustworthiness</b>					
<b>Safe decoding</b>	MOD (2024)	Safety branch	LLaMA-2-13B/70B	—	Logit fusion for safety–utility
<b>Safe decoding</b>	W2S Jailbreaking (2025)	LLaMA-2-13B	LLaMA-2-70B	AdvBench, MaliciousInstruct	Analyze SLM logit effects
<b>Safe decoding</b>	Offset Unlearning (2025a)	LLaMA-2-7B	LLaMA-2-13B	TOFU	Logit offset for unlearning
<b>Safe decoding</b>	LLM Purifying (2024a)	CodeLLaMA-7B	CodeLLaMA-13B	HumanEval, LAMBADA, etc.	Logit fusion for clean gen.
<b>SLM guard</b>	LLaMA Guard (2023)	LLaMA-2-7B	LLaMA-70B	ToxicChat, OpenAI ModEval	I/O safety screening
<b>SLM guard</b>	Prompt Guard / 2 (2024; 2025b)	DeBERTa-v2-22M/86M	LLaMA/GPT-family	Red-teaming (multilingual), etc.	Lightweight input filtering
<b>SLM guard</b>	ShieldGemma / 2 (2024; 2025)	Gemma-2B/9B/27B	Any	ToxicChat, OpenAI Mod, etc.	Fine-grained moderation
<b>SLM guard</b>	WildGuard (2024)	Mistral-7B-v0.3	Any	WildGuardMix	Multi-risk detection
<b>SLM guard</b>	ThinkGuard (2025)	LLaMA-3-8B	Any	BeaverTails, ToxicChat	Reasoned moderation
<b>SLM guard</b>	MiniCheck (2024)	Flan-T5 / UL2	GPT-4 / Claude	LLM-AggrFact	Fact verification

## 2.2 Division–Fusion Collaboration

Division–fusion collaboration paradigm is preferred when multiple models exhibit heterogeneous capabilities and no single backbone model is highly suitable. According to different task needs, this paradigm mainly includes (1) *Parallel Ensemble* for collective intelligence and (2) *Sequential Cooperation* for multi-stage workflows.

### (1) Parallel Ensemble: Collective Intelligence

As shown in Fig. 4, multiple SLMs and LLMs work in parallel, and their outputs are integrated

for higher accuracy. Two common strategies are *majority voting* and *cross-verification*. For *majority voting*, as in ELM (Gondara et al., 2025), multiple independent solutions are sampled from a set of distinct models and combined by consensus to integrate multi-model capabilities. For *cross-verification*, as in CaLM (Hsu et al., 2024), an LLM and an SLM independently generate answers in parallel and iteratively refine both inputs and model states, continuing the process until their outputs reach consensus.

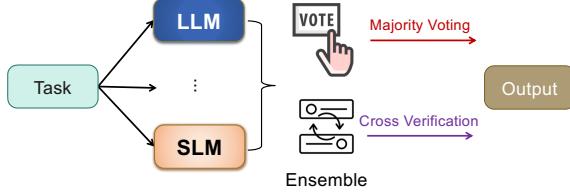


Figure 4: Parallel Ensemble: Collective Intelligence.

**(2) Sequential Cooperation: Division of Labor**  
For multi-stage tasks, subtasks are assigned to suitable models and connected in a pipeline, as shown in Fig. 5. When tasks are explicitly staged, SLMs and LLMs take different roles: SLMs handle precise components (e.g., schema matching in ZeroNL2SQL (Fan et al., 2024) and KDSL (Chen et al., 2025a), question decomposition in Collab-RAG (Xu et al., 2025)), while LLMs manage complex reasoning (e.g., GCIE (Bao and Wang, 2024)). When stages are implicit, the LLM acts as a *planner* and SLMs as *executors*, as in HuggingGPT (Shen et al., 2023) and TrajAgent (Du et al., 2024), which assign subtasks to expert SLMs and integrate them.

### 2.3 Discussion

Current SLM–LLM collaborations for performance highlight the potential of combining specialized and general models but remain limited by fragmented ecosystems and incomplete evaluation standards. Future research should establish open, cross-domain platforms enabling efficient model discovery and integration, alongside collaborative benchmarks that assess structured cooperation, throughput, and cost–performance trade-offs to better capture real-world system efficiency.

## 3 Collaboration for Cost-Effectiveness Trade-off

LLMs deliver advanced performance but face prohibitive costs, including computational expense (FLOPs, GPU hours), high latency, significant communication overhead, large storage footprints, and substantial API spend. Mitigating these costs

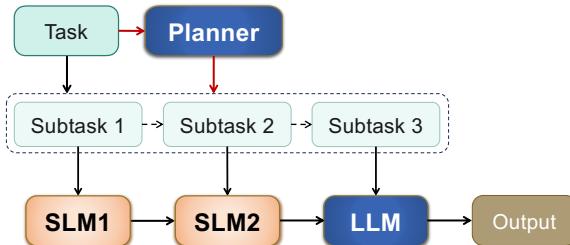


Figure 5: Sequential Cooperation: Division of Labor.

through isolated model optimization is often inefficient and reaches diminishing returns. SLMs offer a compelling pathway to cost-efficiency by serving as lightweight, specialized collaborators (Wang et al., 2025a). This section targets *cost-effectiveness* in SLM–LLM collaboration frameworks, which are organized across the language modeling lifecycle into three stages: (1) *Pre-training Stage*: strategies like teacher-guided data curation and co-curricula use LLMs to guide SLM learning for improved compute and data efficiency; (2) *Tuning stage*: selective knowledge distillation ( $\text{LLM} \rightarrow \text{SLM}$ ) and proxy transfer ( $\text{SLM} \rightarrow \text{LLM}$  warm-starts or adapters) cut adaptation FLOPs and storage while preserving task quality; and (3) *Inference stage*, cascade routing, speculative decoding, and compute-optimal test-time scaling allocate just-enough capacity per query to lower latency, communication, and per-call/API cost.

### 3.1 Collaboration During Pre-Training Stage

The pre-training stage constitutes a computationally intensive phase of the LLM lifecycle, making it a primary target for cost-effectiveness optimization. The challenge lies in achieving high model capability without incurring the prohibitive expense of training on a massive yet low-quality data corpus. SLM–LLM collaboration during the pre-training stage addresses this by employing inter-model guidance to improve data efficiency and optimize the training trajectory. These methods can be categorized into three types: (1) Data curation, where Fig. 6a illustrates an LLM refining data for efficient SLM pre-training, and Fig. 6b shows an SLM evaluating data quality to reduce LLM pre-training cost; (2) Co-curriculum (Fig. 7a), which progressively grows from small to large model capacity; and (3) Pre-training distillation (Fig. 7b), which directly transfers knowledge from a teacher large model to a student small model.

**(1) Data Curation** High-quality data are vital for language model training, yet real-world corpora are often low-quality and noisy. Using low-quality data inflates computational costs and degrades model performance. SLM–LLM collaboration enhances data curation cost-effectively: (1) SLMs select or reshape data for LLM pretraining to boost performance with less data (Fig. 6a); (2) SLMs estimate data quality (e.g., perplexity) to guide LLM pretraining efficiently (Fig. 6b). For instance, the SALT (Rawat et al., 2024) shows that

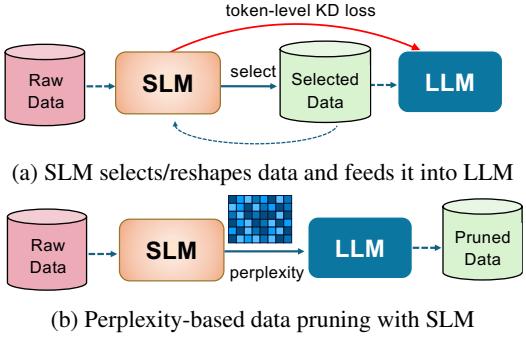


Figure 6: Data Curation.

a compact model can supply soft labels and identify informative hard examples, accelerating large-model pre-training while improving quality, reducing steps, FLOPs, and energy; Conversely, Ankner et al. (2024) adopts perplexity-based filtering with an SLM as the reference scorer to remove low-yield documents/tokens, cutting the optimization steps needed to reach a target loss.

**(2) Co-Curriculum** Training model families efficiently is challenging because large models are costly to start from scratch. Co-curriculum mitigates this through this agenda: pretrain a small model, grow it to a larger one via parameter reuse, then continue training on equal-or-harder data; repeat the grow → train cycle to form a consistent model family across sizes (see Fig. 7a). Growth can be realized in several ways: LIGO (WANG ET AL., 2023B) learns a linear growth operator that maps small-model weights to a larger architecture, where the operator is factorized into width/depth with Kronecker structure before continuing standard training, yielding up to 50% compute savings compared to large-from-scratch while preserving quality. PROGRESSIVE TRAINING (Yano et al., 2025) expands width/depth in stages (e.g., 1B→2B→8B), carrying weights forward and using size-aware schedules that assign higher max LR for smaller models, longer warmup for larger ones, and token allocation that favors stages with

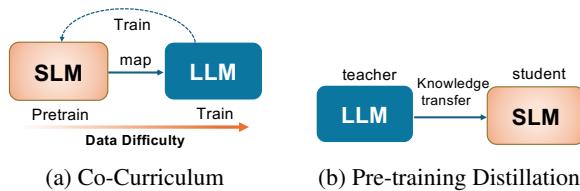


Figure 7: (a) Co-curriculum learning; (b) Knowledge distillation.

higher marginal gain. HYPERCLONING (Samragh et al., 2024) performs a hidden-dimension expansion preserving function by cloning linear layers so that the larger model initially reproduces the smaller model’s logs, producing stable warm starts and substantial savings in GPU-hours compared to cold starts.

**(3) Pre-Training Distillation** Pre-training distillation (PD) transfers knowledge from a teacher LLM to a student SLM through logit matching and data refinement, reducing data requirements while enhancing model capability (see Fig. 7b). Existing works fall into two categories based on the supervision signal: (i) logits-based and (ii) data-based pre-training distillation. For the former, task-agnostic distillation frameworks such as DISTILBERT (Sanh et al., 2019), TINYBERT (Jiao et al., 2020), and MINILM (Wang et al., 2020) transmit teacher logits and embeddings to students as supervision signals. Peng et al. (2025) extend this to larger student LMs, addressing challenges in logits storage, compression, signal design, capacity gap, and online–offline trade-offs. DPT (Goyal et al., 2025) further shows logits-based pre-training distillation enhances test-time scaling but weakens in-context learning, providing analytical insights into this trade-off. For the latter, MINIPLM (Gu et al., 2025) performs offline teacher inference to reshape the pre-training corpus by (a) difficulty reweighting, prioritizing examples with informative teacher signals, and (b) diversity balancing, expanding topical, stylistic, and structural coverage, then trains a compact student on a refined mix.

## 3.2 Collaboration During Tuning Stage

Fine-tuning language models is costly along two fronts: (1) for tuning SLMs, relying on LLM distillation signals during adaptation increases FLOPs or API expenses, and fine-tuning quality depends on supervision quality: poor data wastes both tokens and computation and (2) directly fine-tuning the LLM is expensive in terms of FLOPs, memory, and time. SLM–LLM collaboration mitigates these costs by: (1) *Selective Knowledge Distillation* ( $SLM \Leftarrow LLM$ ) replaces repeated LLM usage with distilled SLMs and increases information per token via selective signals and sampling (Fig. 8); and (2) *Proxy Transfer* ( $SLM \Rightarrow LLM$ ) employs SLMs to produce reusable updates or control signals for efficient LLM adaptation (Figs. 9a and 9b).

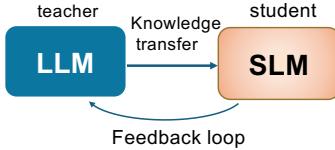


Figure 8: Selective Knowledge Distillation.

**(1) Selective Knowledge Distillation.** Full teacher supervision is costly and often redundant, while selective KD focuses limited guidance where it moves the needle most. We frame selective KD as teacher-in-the-loop curation that minimizes adaptation cost while preserving quality (Fig. 8). The pipeline selects high-yield samples where the teacher is confident but the student is uncertain, shapes supervision beyond hard labels to raise information per token, targets imitation to task-relevant representations instead of uniform mimicry, and then closes the loop using student feedback to guide the next round of teacher queries. In this loop, adaptive selection steers supervision to the error frontier—reducing data and teacher calls (LLKD (Li et al., 2025a); student-in-the-loop selection with retained rationales (Jazbec et al., 2024)); dense yet compact supervision replaces bare labels with short, information-rich signals that clarify boundaries and reasoning—contrastive label refinement (SynCID (Liang et al., 2024)), concise Cot (HAWKEYE (She et al., 2025), and causal explanations for robustness (Muhebwa and Osman, 2025; Lorè et al., 2024)); targeted matching aligns losses with where features live—layers/heads and cross-head logits that carry discriminative structure (C2KD (Chen et al., 2025d)); and behavioral KD distills compact tool-use trajectories to amortize exploration (Agent Distillation (Kang et al., 2025)). Applications instantiate the same loop end-to-end: LLM-assisted candidate generation with on-device ranking (LSC4Rec (Lv et al., 2025)) operationalizes adaptive selection in recommendation systems; latency-sensitive recommenders pair KD with pruning/quantization (Behdin et al., 2025) to shape supervision under strict budgets; lightweight planners distilled via LLM-guided SFT/RL (SmallPlan (Pham et al., 2025)) emphasize targeted matching to task-relevant skills; and “single frozen-LLM prompt, SLM decode” amortization (Bergner et al., 2024) closes the loop by throttling future teacher calls based on student performance—collectively cutting FLOPs, tokens, and LLM calls while retaining near-LLM quality.

**(2) Proxy Transfer** Proxy transfer reduces LLM adaptation costs by using small models as proxies to generate parameters or signals that can be reused by the larger model. This strategy operates through two main pathways: (1) SLMs, often compressed from the LLM, are fine-tuned with low resources to produce LoRA-like updates compatible with the original LLM (Fig. 9a); and (2) fine-tuned SLMs have their outputs merged with those of the LLM, simulating the effect of fine-tuning the large model through a lightweight proxy (Fig. 9b). Both pathways reduce the LLM’s required FLOPs, data, and tuning time. For example, LoRAM (Zhang et al., 2025a) trains low-rank adapters on an SLM to locate effective subspaces, later reused in LLMs. LiteMOE (Zhuang et al., 2024) extracts proxy submodels for on-device tuning, enabling local specialization and feedback propagation. GateKeeper (Rabanser et al., 2025) cascades an SLM and LLM to handle easy cases locally and defer harder ones, cutting inference cost, while G-Boost (Fan et al., 2025c) integrates fine-tuned SLM outputs to refine LLM distributions with minimal updates.

### 3.3 Collaboration During Inference Stage

Inference cost arises from three sources: (i) running large models on *every* request (high FLOPs, latency, or API cost); (ii) decoding inefficiency (token-by-token verification by a single heavy model); and (iii) misallocated compute (overspending on easy queries and underspending on hard ones). SLM–LLM collaboration at the inference stage can address these through: (1) Cascade routing: a lightweight router which is guided using some uncertainty threshold, sending most traffic to a cheap SLM and escalating only when necessary (Fig. 10);

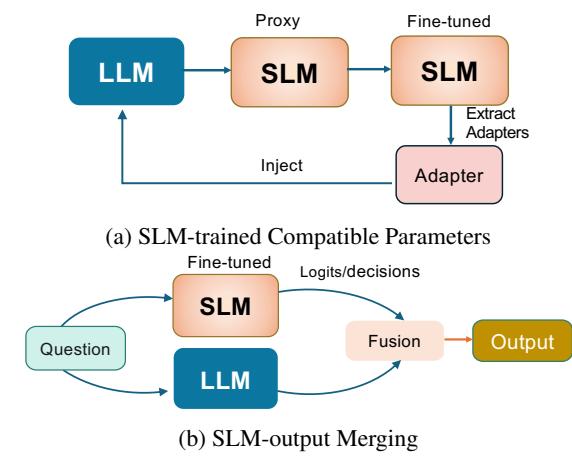


Figure 9: Proxy Transfer.

(2) Speculative decoding: a fast drafter (often an SLM) proposes multiple tokens that a strong verifier (LLM) accepts or corrects in bulk (Fig. 11); and (3) Compute-optimal test-time scaling (TTS): under a fixed budget, optimizes model choice and sampling budgets across SLM/LLM families to meet the target quality (Fig. 12).

**(1) Cascade Routing** Cascade routing reduces average serving costs by directing most requests to a cheap SLM and escalating only complex cases to an LLM. Routers operate at different granularities: (i) query-level for holistic request classification, (ii) token/span-level for fine-grained generation control, and (iii) resource-aware for expert selection under system constraints.

(i) **Query-level routers** make a single deferral decision per input. Classical methods train a lightweight classifier to judge response reliability (Chen et al., 2024a; Ong et al., 2025; Zhang et al., 2024d). Extensions predict query difficulty for adaptive routing (Yue et al., 2024; Hao et al., 2024), including SlimPM (Tan et al., 2024), which uses a slim proxy to detect an LLM’s knowledge gaps and decide when to retrieve.

(ii) **Token/span-level routers** exert finer control by only invoking the LLM for critical tokens or segments. This improves the cost–quality trade-off by letting SLMs handle non-critical generation and LLMs only for critical tokens (e.g., CITER (Zheng et al., 2024) and Roads to Rome (Fu et al., 2025b)).

(iii) **Resource-aware routers** frame model selection as a constrained optimization problem, which uses contextual bandits to pick the best model under latency constraints (Wang et al., 2025c) or use MoE gates to dispatch requests across edge/cloud models, balancing load and budget (Jin et al., 2025).

**(2) Speculative Decoding** Speculative decoding reduces LLM compute by allowing a cheaper drafter to propose tokens (or short continuations) that a stronger verifier accepts in bulk (Fig. 11). Existing studies can be grouped into three major directions: (i) adaptive draft–verify pipelines, (ii) system- and hardware-aware parallelization, and

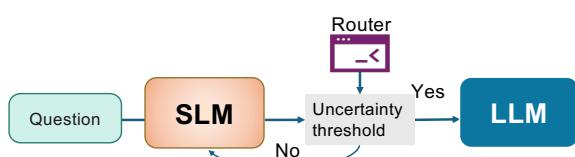


Figure 10: Cascade Routing.



Figure 11: Speculative Decoding.

(iii) distributed and hierarchical multi-model collaboration.

(i) **Adaptive Draft–Verify Pipelines** Early frameworks such as speculative decoding (Leviathan et al., 2023; Chen et al., 2023) and SpecDec (Xia et al., 2023) establish the draft–then–verify paradigm, where SLMs propose multi-token drafts and LLMs verify them in parallel for speedups. BiLD (Kim et al., 2023), staged SD (Spector and Re, 2023), and LLMcad (Xu et al., 2023) extend this idea to big-little or on-device settings with rollback and correction strategies. Later methods including SpecInfer (Miao et al., 2024), cascade SD (Chen et al., 2024b), and SpecTr (Sun et al., 2023), introduce tree- or cascade-based verification, while online SD (Liu et al., 2024c), TurboSpec (Liu et al., 2024b), SCD (Yuan et al., 2024), and mixture-of-attentions SD (Zimmer et al., 2024) add adaptive retraining, feedback control, and enhanced drafting accuracy. Together, these approaches evolve SD into dynamic, feedback-driven pipelines that balance quality and efficiency.

(ii) **System- and Hardware-Aware Parallelization** Several systems accelerate SD through pipeline and hardware optimization. EdgeLLM (Xu et al., 2024b), SpecExec (Svirchevski et al., 2024), and SPIN (Chen et al., 2025b) boost throughput via multi-token speculation, GPU pipelining, and heterogeneous SLM selection, while Dovetail (Zhang et al., 2024g) and APD (Israel et al., 2025) exploit heterogeneous devices and adaptive speculative width. Hardware-level efforts like HADES (Yang et al., 2025) embed SD primitives into accelerators, and HiSpec (Kumar et al., 2025) uses early-exit layers and cache reuse for lightweight intermediate verification. These methods make SD a pipeline-optimized, hardware-co-designed inference paradigm.

(iii) **Distributed and Hierarchical Multi-Model Collaboration** Edge–cloud and multi-agent extensions broaden SD into large-scale collaboration. Fast edge–cloud SD (Venkatesha et al., 2025), SLED (Li et al., 2025e), and heterogeneous SD frameworks (Zhu et al., 2025) distribute drafting to edge SLMs and verification to cloud LLMs using asynchronous batching. SpecServe (Huang

et al., 2025b) and CoSine (Gao et al., 2025a) add adaptive schedulers and confidence-prior verifiers for SLO-aware efficiency, while PICE (Zhan et al., 2025) and CoS (Fu et al., 2025a) extend SD to semantic-level and multi-model collaboration through dynamic task routing and alternating proposer–verifier roles. Together, these systems turn SD into a distributed orchestration framework for scalable, low-cost LLM inference.

**(3) Compute-optimal Test-time Scaling** Test-Time Scaling (TTS) increases inference compute to improve performance, while compute-optimal TTS maximizes it under fixed budgets by selecting suitable model sizes and families, representing a form of SLM–LLM collaboration. BestRoute (Ding et al., 2025) optimizes model routing and TTS sampling budgets to reduce cost, and AgentTTS (Wang et al., 2025b) extends this to multi-stage tasks through dynamic model and budget allocation.

### 3.4 Discussion

Existing cost-effectiveness collaborations demonstrate clear savings across compute, latency, communication, storage, and API costs by coordinating the ML lifecycle but remain limited by fragmented pipelines, inconsistent cost reporting, and brittle rules for determining when to hand off to the LLM (Behera et al., 2025). Future work should standardize end-to-end cost-effectiveness metrics and employ adaptive routing, paired with compression, bidirectional distillation, and related techniques, to ensure reliable savings across SLM–LLM collaboration paradigms.

## 4 Privacy-preserving Cloud–Edge Collaboration

Deploying LLMs on edge devices is limited by hardware constraints. A practical alternative is a cloud–edge framework where lightweight SLMs handle local, context-aware tasks, and cloud-based LLMs provide broader generalization (Lv et al., 2023; Shao et al., 2025). However, transmitting sensitive data from trusted edge SLMs to semi-trusted cloud LLMs raises privacy concerns, as

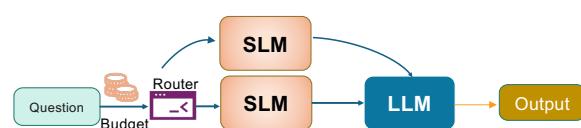


Figure 12: Compute-optimal TTS.

personally identifiable or proprietary information may be logged and leaked for training (Duan et al., 2023), posing long-term data security risks.

To balance privacy and performance, privacy-preserving cloud–edge collaboration has emerged at both the inference and fine-tuning stages. At the *inference stage*, SLMs act as (1) Sensitive Information Gatekeepers, filtering or anonymizing data before sending it to LLMs, or as (2) All-Information Guardians, retaining private context locally and integrating it after generation. At the *fine-tuning stage*, collaboration occurs via (1) SLMs as Learners (learning from LLMs via distillation), (2) LLMs as Learners (adapting via proxy tuning using SLM signals), or (3) Collaborative Learners (jointly improving through federated knowledge transfer).

### 4.1 Inference Stage

During inference, edge user requests may contain sensitive information. Edge SLMs can process locally but with lower quality than cloud LLMs, while direct cloud LLM use risks data exposure. Thus, privacy-preserving edge–cloud collaboration is needed, based on protection levels, categorized into (1) Sensitive Information Gatekeepers (Fig. 13) and (2) All-Information Guardians (Fig. 14).

#### (1) SLMs as Sensitive Information Gatekeepers

To protect sensitive information in edge–cloud collaboration, the edge SLM serves as a privacy-preserving filter, for (i) sanitizing sensitive content and (ii) selectively disclosing necessary information before transmitting requests to the cloud.

**(i) Sanitizing sensitive information:** Fig. 13(a) shows how SLMs remove or rephrase prompts containing personally identifiable information (PII). Casper (Chong et al., 2024) use an SLM to filter PII before cloud transmission, while Papadopoulou et al. (2022) employ SLM probabilities for detection. LLM gatekeeper (Uzor et al., 2025) rephrases queries to preserve meaning while removing PII,

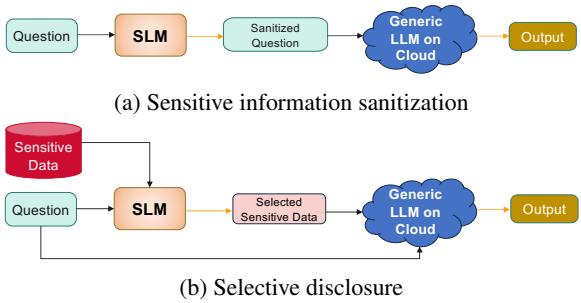


Figure 13: SLMs as Sensitive-Information Gatekeepers.

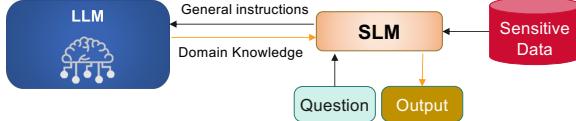


Figure 14: SLMs as All-Information Guardians.

applied to clinical data (Wiest et al., 2024). Hartmann et al. (2024) enhance SLMs by masking sensitive data and using LLM-generated examples.

(ii) **Selective disclosure:** Fig. 13(b) illustrates selective disclosure, where the edge SLM shares limited, task-relevant information to reduce privacy risks. CoGenesis (Zhang et al., 2024f) shares sketches or logits with the LLM, while CORE (Fan et al., 2025a) ranks and filters relevant context. P<sup>3</sup>Defer (Zhang et al., 2024d) employs a policy network to balance privacy and quality, and RemoteRAG (Cheng et al., 2025) enforces a differential privacy budget to mathematically bound potential leakage. In sum, these methods shift from full-text disclosure to abstracted representation sharing, mitigating data exposure in SLM–LLM collaboration.

**(2) SLMs as All-Information Guardians** Edge device policies may impose strict privacy requirements that prohibit any PII disclosure. Under such constraints, edge SLMs act as *All-Information Guardians*, processing sensitive data entirely on-device while integrating cloud LLM knowledge, ensuring that private information never leaves the user’s control, as shown in Fig. 14. Sketch-based CoGenesis (Zhang et al., 2024f) exemplifies the paradigm, using the cloud LLM for high-level planning while the SLM personalizes results locally with user logs. PrivacyBoost-SLM (Zhang et al., 2024i) applies this to clinical decision-making, combining cloud-derived medical knowledge with patient data. RemoteRAG (Cheng et al., 2025) extends this idea by pairing SLMs with local retrievers (RAG) to integrate private and domain-general knowledge without exposing raw data. Hartmann et al. (2024) further employ LLMs as RAG example providers to enhance the SLM context. Industrial systems such as Apple Intelligence (Gunter et al., 2024) adopt a similar approach, processing sensitive data on-device and sending only abstracted information to the cloud.

## 4.2 Fine-tuning Stage

During fine-tuning, edge data can facilitate the evolution of both edge and cloud LLMs by providing valuable fine-tuning signals. However, ensuring

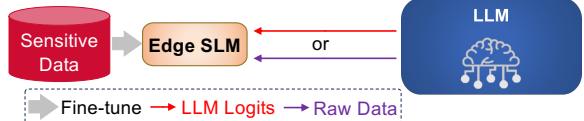


Figure 15: SLMs as Learners.

data protection without exposing sensitive information to the cloud remains a major challenge. To address this, privacy-preserving edge–cloud training frameworks have been proposed, which can be categorized into three paradigms based on the learning target: (1) SLMs as Learners: the edge SLM acquires new capabilities from larger LLMs through local fine-tuning, distillation, or personalization, guided by cloud LLMs without revealing raw data (Fig. 15); (2) LLMs as Learners: the cloud LLM improves by consuming proxy signals or adapters distilled from locally trained SLMs, thereby enhancing generalization without accessing private data (Fig. 16); and (3) Collaborative Learners: both SLMs and LLMs co-evolve through federated or privacy-preserving coordination (Fig. 17).

**(1) SLMs as Learners** Fig. 15 shows edge SLMs learning from cloud LLMs to improve their ability and reduce cloud dependence through subsequent local fine-tuning. SLMs can learn via two modes: (i) raw text, such as reasoning traces or samples, and (ii) feedback logits as supervision signals.

(i) **Raw Data:** SLMs enhance reasoning by learning from cloud LLM outputs while keeping private data local. The LLM provides interpretable supervision (e.g., responses, reasoning traces) or synthetic samples for SLM fine-tuning. MiniLLM (Gu et al., 2024) and LlamaDuo (Park et al., 2025) distill reasoning traces, while DRAG (Chen et al., 2025c) extends to retrieval-augmented reasoning. Privacy-aware frameworks such as HomeLLaMA (Huang et al., 2025c) and Qin et al. (2024) use selective textual supervision to align SLMs with user preferences under strict privacy constraints.

(ii) **Logit-based Learning:** SLMs learn from teacher LLMs’ numerical outputs, using logits as soft targets to imitate their decision boundaries without accessing raw text. TinyLLM (Tian et al., 2025) distills from multiple teachers for robustness, Mix Distillation (Li et al., 2025g) combines LLM and SLM supervision, and ADPA (Gao et al., 2025b) introduces an advantage-based objective for better reasoning alignment, ensuring privacy and efficiency through abstracted signal exchange.

**(2) LLMs as Learners** LLMs can be adapted to sensitive data without direct access by leveraging an edge SLM tuned locally. The SLM forwards only supervision signals, such as (i) logits or (ii) LoRA signals, to the LLM, enabling privacy-preserving alignment, as shown in Fig. 16.

*(i) Logit-based Learning:* Instead of directly fine-tuning an LLM, Ormazabal et al. (2023) demonstrate that an LLM can be steered by tuning an SLM on private data and exposing only the SLM’s output logits to guide the LLM’s responses. Specifically, they train a lightweight MLP on the logits produced by both the SLM and the LLM, which is then used to steer the LLM’s output during inference. This approach enables the use of private data for adaptation while avoiding its direct exposure to the LLM. An extension of this method involves applying direct logit offsets between the tuned model and the LLM (Liu et al., 2024a; Wang et al., 2025d), by computing the logits difference between the trained SLM and its frozen counterpart. The LLM adds this offset to its own output logits during inference.

Follow-up work has examined the limitations of this approach. CPT (He et al., 2024) and GradOT (Yao et al., 2025) address inconsistencies arising from discrepancies between training and inference pipelines. Whereas the SLM is trained alone, it is expected to interact with its frozen counterpart to compute the logits offset and steer the LLM during inference. To address this gap and improve alignment, CPT integrates both the frozen SLM and LLM in the training process to closely mirror the inference phase interaction and include the LLM feedback in the gradient updates. On the other hand, GradOT approximates the gradient updates using offsite-tuning (Xiao et al., 2023) to enable efficient alignment without co-training. To enhance robustness, GOOD (Fang et al., 2024a) decodes the SLM’s output into text and re-encodes it for the LLM to extend logit steering to SLM–LLM pairs without a shared vocabulary.

*(ii) LoRA-based Learning:* Recent work leverages LoRA signals to propagate knowledge instead of requiring logit outputs from SLMs to

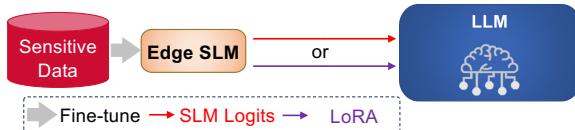


Figure 16: LLMs as Learners.

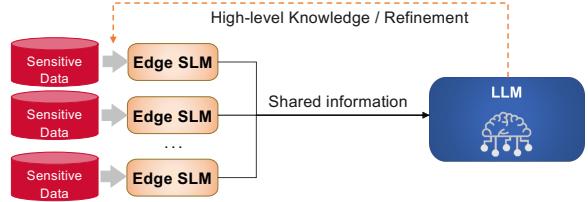


Figure 17: Cloud-Edge Collaborative Learning.

enable adaptation without direct access to private data. LoRASuite (Li et al., 2025f) and LoRA-X (Farhadzadeh et al., 2025) demonstrate how LoRA signal transfer can be applied across model versions and architectures. Similarly, TransLoRA (Wang et al., 2024c) and Cross-LoRA (Xia et al., 2025) extend this capability to heterogeneous model families, enabling more generalizable and privacy-conscious adaptation of LLMs.

**(3) SLMs and LLMs as Collaborative Learners** Beyond one-way transfer, collaboration can be bidirectional: SLMs and LLMs co-adapt via shared representations, logits, or adapter weights while preserving privacy. Fig. 17 shows multiple edge SLMs learn from local private data and transmit abstracted updates, such as logits or LoRA adapters, to the cloud LLM for aggregation and refinement, and then the cloud LLM returns high-level knowledge or refinement feedback to the local. CrossLM (Deng et al., 2025) achieves mutual enhancement by combining private task data and LLM-generated samples for privacy-preserving co-training. LSRP (Zhang et al., 2025c) enables bidirectional feedback, where the LLM guides SLM retrieval and refines its own responses. Federated frameworks such as FedMKT (Fan et al., 2025b), FedPT (Gao et al., 2024), FedPFT (Peng et al., 2024), FDLoRA (QI et al., 2024), and the Automated Federated PEFT Pipeline (Fang et al., 2024b) aggregate client-side SLM adapters or logits to update central LLMs while preserving data privacy. FLoRA (Wang et al., 2024e) further improves personalization through enhanced edge aggregation.

### 4.3 Discussion

Current cloud–edge SLM–LLM collaborations face challenges in achieving secure peer-to-peer exchange, effective cold-start learning, formal privacy guarantees, and scalable personalization under strict data protection. Future work should develop adaptive frameworks enabling privacy-preserving collaboration and lightweight personalization for

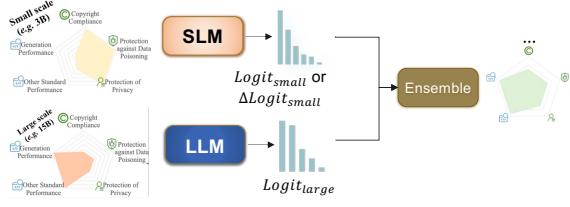


Figure 18: SLM Guided Safe LLM Decoding.

policy-compliant intelligence in sensitive domains such as healthcare and customer service.

## 5 Collaboration for Trustworthiness

LLMs offer strong generative ability and broad knowledge coverage but face major trustworthiness challenges in real-world use. Uncontrolled training data can lead to hallucinations, harmful or biased outputs, privacy leaks, and vulnerabilities exploitable through jailbreaks or adversarial attacks (Zhang et al., 2025d; Liu et al., 2023; Wu et al., 2025; Zhang et al., 2025b; Liu et al., 2020; Wang et al., 2021). Updating LLMs for safety is costly and may harm generation quality. A more practical solution is integrating *safety policies* that guide generation without retraining. SLMs serve this role effectively due to their compactness, independence from LLM architectures, and ease of policy updates. Recent SLM–LLM collaborations use SLMs to encode or enforce safety policies while LLMs handle content generation. Two paradigms dominate: (1) *Safety-guided decoding*, where an SLM modifies LLM logits during decoding for token-level control; and (2) *Guardian–generator*, where the SLMs trained as Guardians filter inputs and audit outputs, providing interaction-level governance. These paradigms are shown in Figs. 18 and 19.

### 5.1 Safety-Guided Decoding

Unsafe outputs in LLMs often arise during decoding; thus, integrating safety policies into token-level generation is crucial yet challenging, as it is difficult to anticipate which tokens may trigger unreliable content. Recent studies employ safety-tuned SLMs, fine-tuned for risks such as jailbreaks, privacy leaks, or bias, to guide LLM decoding in a safety-aware manner. As shown in Fig. 18, SLM and LLM logits are fused to ensure both quality and safety through two strategies: (1) direct logit fusion (linear combination) and (2) logit offset fusion (using SLM logits as offsets to steer LLM probabilities toward safer tokens).

**(1) Direct Logit Fusion** The CP- $\Delta$  theory (Vyas et al., 2023) provides an information-theoretic foundation for model fusion, demonstrating that combining the predictive distributions of two models,  $q_1(y|x)$  and  $q_2(y|x)$ , with distinct copyright risks yields a fused distribution  $p(y|x) \propto q_1(y|x)^\alpha q_2(y|x)^{1-\alpha}$  that minimizes weighted KL divergence and balances their strengths without retraining, where  $\alpha$  controls each model’s contribution. The fused distribution lies closer to both sources than they are to each other, thus achieving a purification effect, retaining desirable properties while reducing copyrighted content. This operation is equivalent to linear weighting in logit space,  $z_p = \alpha z_1 + (1 - \alpha) z_2$ , providing the theoretical foundation for SLM–LLM collaborative logit fusion. Subsequent methods build on this principle: Purifying LLMs (Li et al., 2024a) fuses clean SLM and contaminated LLM logits to mitigate copyright, privacy, and backdoor risks, while MOD (Shi et al., 2024) extends fusion to multiple objectives, integrating models optimized for fluency, faithfulness, and safety to enable controllable generation.

**(2) Logit Offset Fusion** Mitchell et al. (2024) introduced the concept of logit offset fusion by decomposing a fine-tuned model’s output into the base model’s logits and a behavioral delta:

$$z_{\text{ft}}(x) = z_{\text{base}}(x) + \Delta(x), \quad (1)$$

where  $\Delta(x)$  represents the *behavioral delta* induced by fine-tuning. Through an *up-scaling* strategy, it integrates a large pre-trained model’s logits  $z_{\text{large}}$  with the behavioral delta of a small fine-tuned model  $\Delta(x) = z_{\text{ft}}(x) - z_{\text{small}}(x)$ :

$$z_{\text{fusion}}(x) = z_{\text{large}}(x) + \lambda \Delta(x), \quad (2)$$

where  $\lambda$  is a scaling factor aligning the magnitude of the small model’s delta with the large model’s logit scale. This simple logit-level combination achieves up to 73% of the full large-model fine-tuning helpfulness without re-training the large model. This demonstrates that safety-aligned small models’ behavioral deltas can enhance LLM safety when fused at the logit level. Building on this idea, Offset Unlearning (Huang et al., 2025a) trains SLMs to generate targeted logit offsets that suppress sensitive or fabricated knowledge for privacy-preserving unlearning. Conversely, Weak-to-Strong Jailbreak (Zhao et al., 2025) reveals that unsafe SLMs can steer safe LLMs toward harmful

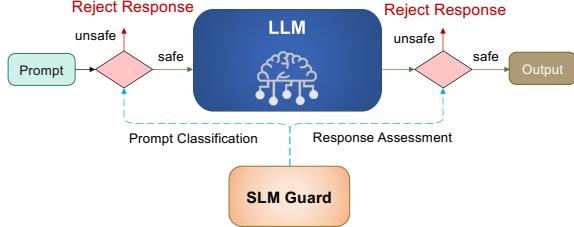


Figure 19: SLM Guardian, LLM Generator.

outputs, implying that the same mechanism can defensively employ safe SLMs to counter jailbreak attacks through safety-guided logit fusion.

## 5.2 SLM as Guardian, LLM as Generator

Guardrail-based approaches enhance LLM safety by placing SLMs before and after generation. In the SLM-as-Guardian and LLM-as-Generator paradigm, as shown in Fig. 19, SLMs, encoding the safety policy, handle input filtering and output auditing, offering configurable, interpretable, and reusable safety control across evolving applications.

Building on this paradigm, later studies advanced the framework. Llama Guard (Inan et al., 2023) built a bidirectional safety pipeline using a fine-tuned LLaMA-2-7B classifier. Llama Guard 2 (Team, 2024) added multi-label risk classification; Llama Guard 3 (Dubey et al., 2024) expanded multilingual support and inspired lightweight variants like Llama Guard 3-1B-INT4 (Fedorov et al., 2024) and cross-modal Llama Guard 3 Vision (Chi et al., 2024). Llama Guard 4 (AI, 2025a) further refined the taxonomy to 14 safety categories and was adapted for healthcare auditing (Gangavarapu, 2024). For lightweight protection, Prompt Guard (AI, 2024) and Prompt Guard 2 (AI, 2025b), based on DeBERTa-v2 (He et al., 2021), serve as fast, low-cost input filters. ShieldGemma (Zeng et al., 2024, 2025) and WildGuard (Han et al., 2024) use synthesized, large safety data to boost robustness against adversarial prompts. ThinkGuard (Wen et al., 2025) adds “slow thinking” for better interpretability and defense. Beyond text safety, MiniCheck (Tang et al., 2024) applies the guardian concept to factual verification, while Cascade Guardrails (Nagireddy et al., 2024) explores hierarchical defenses. LlamaFirewall (Chennabasappa et al., 2025) extends this paradigm to multi-agent settings.

## 5.3 Discussion

Current SLM–LLM collaborations for trustworthiness face challenges in unifying decoding and guarding, extending safety beyond text, enabling edge deployment, and standard evaluation. Future work should build integrated frameworks with multimodal safety, lightweight edge guardians, and standard evaluation benchmarks.

## 6 Applications

We summarize the representative works in Table 1, detailing their collaboration mechanisms, employed SLMs and LLMs, evaluation datasets, and goals. From these studies, we can summarize the applications under each category.

**Collaboration for performance** In guidance-generation, SLMs assist LLMs in reasoning and classification tasks, such as intent detection (Liang et al., 2024), natural language inference (Xu et al., 2024a), sentiment analysis (Mojarradi et al., 2024), and multi-hop question answering (Lee et al., 2024). In division–fusion, they form multi-stage pipelines for domains such as clinical analysis (Gondara et al., 2025), factual verification (Hsu et al., 2024), NL2SQL (Fan et al., 2024), and trajectory modeling (Du et al., 2024), where SLMs handle subtasks and LLMs integrate the results. This suggests that guidance-enhanced generation is more suitable for common general-domain tasks, where LLMs are the backbone generator and SLMs are trained on local downstream data, while division–fusion collaboration is preferred when both models exhibit comparable capabilities across different subtasks.

**Collaboration for cost-effectiveness** The cost-effective SLM–LLM collaboration methods show stage-specific application preferences. Pre-training–stage frameworks target corpus construction and scaling efficiency on large datasets (e.g., Pile, FineWeb-Ed, C-Eval), supporting sustainable and scalable model development (Rawat et al., 2024; Yano et al., 2025; Goyal et al., 2025). Fine-tuning–stage methods focus on intent classification and reasoning transfer (e.g., BANKING, CLINC, MMLU, GSM8K), enabling smaller models to inherit LLM capabilities with minimal cost (Jazbec et al., 2024; Zhang et al., 2025a; Fan et al., 2025c). Inference–stage approaches emphasize real-time reasoning and conversational tasks (e.g., AIME, GPQA, ShareGPT) where latency and compute ef-

ficiency are critical (Chen et al., 2024a; Ong et al., 2025; Zhang et al., 2024d).

**Collaboration for cloud-edge privacy** The inference-stage methods are particularly suited for end-user scenarios where privacy is a main concern. Edge SLMs prevent leakage of PII or sensitive context to external providers (Chong et al., 2024; Zhang et al., 2024f), supporting domains such as healthcare and customer service. Depending on privacy needs, SLMs as Information Gatekeepers may be applied (Zhang et al., 2024i; Cheng et al., 2025). Meanwhile, proxy tuning enables domain-specific or personalized LLM adaptation without exposing private data, offering broader potential under edge resource privacy constraints and edge SLMs’ limited reasoning and context capacity (Li et al., 2025f; Wang et al., 2025d; Deng et al., 2025).

**Collaboration for trustworthiness** SLM–LLM collaboration for trustworthiness is applied in safety-critical and compliance-sensitive contexts. Safe decoding methods can correct hallucination, privacy, and toxicity risks in code generation, instruction following, and dialogue by steering the decoding distributions (Li et al., 2024a,a; Mitchell et al., 2024; Huang et al., 2025a). Guardian frameworks support content moderation, assistants, and fact verification by filtering directly unsafe inputs and ensuring output reliability (Inan et al., 2023; AI, 2024; Zeng et al., 2024; Wen et al., 2025). This suggests that the former is better suited for applications requiring a balance between output quality and truthfulness, whereas the latter is preferred for highly secure applications that eliminate potentially risky inputs and outputs.

## 7 Challenges and Future Directions

**Open and Interoperable SLM–LLM Ecosystem** Current SLM–LLM collaborations remain fragmented, with isolated models and task-specific systems limiting interoperability and reuse. Future research should develop open, cross-domain ecosystems that unify specialized and general models through standardized interfaces and shared repositories, enabling efficient model discovery, seamless composition, and collaborative benchmarking across diverse applications and domains.

**Benchmark Design for SLM–LLM Collaboration** Current SLM–LLM evaluations focus mainly on open-ended tasks and performance, overlooking structured tasks and system-level metrics. Future

research should develop diverse benchmarks covering structured reasoning, modular cooperation, and system-level metrics, such as throughput, latency, and cost–performance, to better capture collaborative efficiency and real-world applicability.

**Synergistic SLMs as Decoders and Guardians.** Current safety mechanisms often separate decoding control from post-hoc moderation, limiting effectiveness in SLM–LLM safety collaboration. Future research should develop unified frameworks where SLMs function simultaneously as safety-aware decoders and guardians, enabling multi-stage, end-to-end safety governance that enhances trustworthiness across both generation and interaction phases.

**Cost-Aware SLM–LLM Collaboration** Current SLM–LLM collaborations emphasize performance over cost modeling, risking inefficient resource use. Future work should develop adaptive orchestration frameworks to optimize cost–performance trade-offs through predictive cost-aware routing, non-myopic collaboration policies considering long-term budgets, and multi-objective optimization balancing accuracy, latency, and financial cost for sustainable, scalable SLM–LLM systems.

**Theory for Privacy-Preserving Collaboration** Current privacy-preserving SLM–LLM collaborations lack formal theoretical foundations, relying mostly on empirical evaluations without quantifiable privacy assurances. Future research should establish rigorous metrics and provable bounds for data leakage and privacy preservation, enabling verifiable guarantees of data security and fostering trust in privacy-sensitive SLM–LLM systems.

## 8 Conclusions

In this paper, we present a systematic survey of SLM–LLM collaboration from the perspective of collaboration objectives: performance enhancement, cost-effectiveness, cloud–edge privacy, and trustworthiness. We analyze representative methods showing that most leverage SLMs’ lightweight adaptability. We aim to highlight the current research state and provide insights for future work in this promising area of SLM–LLM collaboration.

## Limitations

Although our work introduces a systematic framework for analyzing SLM–LLM collaboration, several limitations remain. First, given the rapid evolution of language model technologies, certain implicit forms of SLM–LLM collaboration may not

yet be fully captured, and further insights from the research community are encouraged to complement this study. Second, overlaps exist among several collaboration objectives, for instance, the personalization synergy, while not addressed in this survey, often intersects with cloud–edge collaboration, yet these cross-objective studies remain limited despite their conceptual and practical significance. We expect that addressing these challenges will motivate future comprehensive surveys and deeper investigations into SLM–LLM collaboration.

## References

- Meta AI. 2024. Prompt-guard-86m. <https://huggingface.co/meta-llama/Prompt-Guard-86M>. Accessed: 2025-10-03.
- Meta AI. 2025a. Llama guard 4-12b. <https://huggingface.co/meta-llama/Llama-Guard-4-12B>. Accessed: 2025-10-03.
- Meta AI. 2025b. Llama-prompt-guard-2. <https://huggingface.co/meta-llama/Llama-Prompt-Guard-2-86M>. Accessed: 2025-10-03.
- Ali Al-Lawati, Jason Lucas, Zhiwei Zhang, Prasenjit Mitra, and Suhang Wang. 2025. Graph-based molecular in-context learning grounded on morgan fingerprints. *Preprint*, arXiv:2502.05414.
- Zachary Ankner, Cody Blakeney, Kartik Sreenivasan, Max Marion, Matthew L Leavitt, and Mansheej Paul. 2024. Perplexed by perplexity: Perplexity-based data pruning with small reference models. *arXiv preprint arXiv:2405.20541*.
- Mari Ashiga, Wei Jie, Fan Wu, Vardan Voskanyan, Fateme Dinmohammadi, Paul Brookes, Jingzhi Gong, and Zheng Wang. 2025. Ensemble learning for large language models in text and code generation: A survey. *arXiv preprint arXiv:2503.13505*.
- K Bao and Ning Wang. 2024. General collaborative framework between large language model and experts for universal information extraction. In *Findings of the Association for Computational Linguistics: EMNLP 2024*, pages 52–77.
- Kayhan Behdin, Yun Dai, Ata Fatahibaarzi, Aman Gupta, Qingquan Song, Shao Tang, Hejian Sang, Gregory Dexter, Sirou Zhu, Siyu Zhu, and 1 others. 2025. Efficient ai in practice: Training and deployment of efficient llms for industry applications. *arXiv preprint arXiv:2502.14305*.
- Adarsh Prasad Behera, Jaya Prakash Champati, Roberto Morabito, Sasu Tarkoma, and James Gross. 2025. Towards efficient multi-ilm inference: Characterization and analysis of ilm routing and hierarchical techniques. *arXiv preprint arXiv:2506.06579*.
- Andrew Bell. 2025. Less can be more: An empirical evaluation of small and large language models for sentence-level claim detection. In *Proceedings of the Eighth Fact Extraction and VERification Workshop (FEVER)*, pages 85–90, Vienna, Austria. Association for Computational Linguistics.
- Benjamin Bergner, Andrii Skliar, Amelie Royer, Tijmen Blankevoort, Yuki Asano, and Babak Ehteshami Bejnordi. 2024. Think big, generate quick: Llm-to-slm for fast autoregressive decoding. *arXiv preprint arXiv:2402.16844*.
- Tianle Cai, Yuhong Li, Zhengyang Geng, Hongwu Peng, Jason D Lee, Deming Chen, and Tri Dao. 2024. Medusa: Simple llm inference acceleration framework with multiple decoding heads. In *International Conference on Machine Learning*, pages 5209–5235. PMLR.
- Nicholas Carlini, Florian Tramer, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Ulfar Erlingsson, and 1 others. 2021. Extracting training data from large language models. In *30th USENIX security symposium (USENIX Security 21)*, pages 2633–2650.
- Bin Chen, Yu Zhang, Hongfei Ye, Yizi Huang, and Hongyang Chen. 2025a. Knowledge-decoupled synergistic learning: An mlm based collaborative approach to few-shot multimodal dialogue intention recognition. In *Companion Proceedings of the ACM on Web Conference 2025*, pages 3044–3048.
- Charlie Chen, Sebastian Borgeaud, Geoffrey Irving, Jean-Baptiste Lespiau, Laurent Sifre, and John Jumper. 2023. Accelerating large language model decoding with speculative sampling. *arXiv preprint arXiv:2302.01318*.
- Fahao Chen, Peng Li, Tom H Luan, Zhou Su, and Jing Deng. 2025b. Spin: Accelerating large language model inference with heterogeneous speculative models. In *IEEE INFOCOM 2025-IEEE Conference on Computer Communications*, pages 1–10. IEEE.
- Jennifer Chen, Aidar Myrzakhan, Yaxin Luo, Hasaan Muhammad Khan, Sondos Mahmoud Bsharat, and Zhiqiang Shen. 2025c. DRAG: Distilling RAG for SLMs from LLMs to transfer knowledge and mitigate hallucination via evidence and graph-based distillation. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 7240–7260, Vienna, Austria. Association for Computational Linguistics.
- Lihu Chen and Gaël Varoquaux. 2024. What is the role of small models in the ilm era: A survey. *arXiv preprint arXiv:2409.06857*.
- Lingjiao Chen, Matei Zaharia, and James Zou. 2024a. FrugalGPT: How to use large language models while reducing cost and improving performance. *Transactions on Machine Learning Research*.

- Xiao Chen, Changyi Ma, Wenqi Fan, Zhaoxiang Zhang, and Li Qing. 2025d. C2kd: Cross-layer and cross-head knowledge distillation for small language model-based recommendation. In *Findings of the Association for Computational Linguistics: ACL 2025*, pages 17827–17838.
- Ziyi Chen, Xiaocong Yang, Jiacheng Lin, Chenkai Sun, Kevin Chang, and Jie Huang. 2024b. Cascade speculative drafting for even faster llm inference. *Advances in Neural Information Processing Systems*, 37:86226–86242.
- Yihang Cheng, Lan Zhang, Junyang Wang, Mu Yuan, and Yunhao Yao. 2025. **RemoteRAG: A privacy-preserving LLM cloud RAG service**. In *Findings of the Association for Computational Linguistics: ACL 2025*, pages 3820–3837, Vienna, Austria. Association for Computational Linguistics.
- Sahana Chennabasappa, Cyrus Nikolaidis, Daniel Song, David Molnar, Stephanie Ding, Shengye Wan, Spencer Whitman, Lauren Deason, Nicholas Doucette, Abraham Montilla, and 1 others. 2025. Llamafirewall: An open source guardrail system for building secure ai agents. *arXiv preprint arXiv:2505.03574*.
- Jianfeng Chi, Ujjwal Karn, Hongyuan Zhan, Eric Smith, Javier Rando, Yiming Zhang, Kate Plawiak, Zacharie Delpierre Coudert, Kartikeya Upasani, and Mahesh Pasupuleti. 2024. Llama guard 3 vision: Safeguarding human-ai image understanding conversations. *arXiv preprint arXiv:2411.10414*.
- Chun Jie Chong, Chenxi Hou, Zhihao Yao, and Seyed Mohammadjavad Seyed Talebi. 2024. **Casper: Prompt Sanitization for Protecting User Privacy in Web-Based Large Language Models**. *arXiv preprint ArXiv:2408.07004 [cs]*.
- Yongheng Deng, Ziqing Qiao, Ye Zhang, Zhenya Ma, Yang Liu, and Ju Ren. 2025. Crosslm: A data-free collaborative fine-tuning framework for large and small language models. In *Proceedings of the 23rd Annual International Conference on Mobile Systems, Applications and Services*, pages 124–137.
- Dujian Ding, Ankur Mallick, Shaokun Zhang, Chi Wang, Daniel Madrigal, Mirian Del Carmen Hipolito Garcia, Menglin Xia, Laks V. S. Lakshmanan, Qingyun Wu, and Victor Rühle. 2025. **BEST-route: Adaptive LLM routing with test-time optimal compute**. In *Forty-second International Conference on Machine Learning*.
- Yuwei Du, Jie Feng, Jie Zhao, Jian Yuan, and Yong Li. 2024. Trajagent: An llm-based agent framework for automated trajectory modeling via collaboration of large and small models. *arXiv preprint arXiv:2410.20445*.
- Haonan Duan, Adam Dziedzic, Mohammad Yaghini, Nicolas Papernot, and Franziska Boenisch. 2023. On the privacy risk of in-context learning. In *The 61st Annual Meeting Of The Association For Computational Linguistics*.
- Abhimanyu Dubey, Abhinav Jauhri, Abhinav Pandey, Abhishek Kadian, Ahmad Al-Dahle, Aiesha Letman, Akhil Mathur, Alan Schelten, Amy Yang, Angela Fan, and 1 others. 2024. The llama 3 herd of models. *arXiv e-prints*, pages arXiv–2407.
- Gucongcong Fan, Chaoyue Niu, Chengfei Lyu, Fan Wu, and Guihai Chen. 2025a. Core: Reducing ui exposure in mobile agents via collaboration between cloud and local llms. In *Advances in Neural Information Processing Systems (NeurIPS)*.
- Ju Fan, Zihui Gu, Songyue Zhang, Yuxin Zhang, Zui Chen, Lei Cao, Guoliang Li, Samuel Madden, Xiaoyong Du, and Nan Tang. 2024. Combining small language models and large language models for zero-shot nl2sql. *Proceedings of the VLDB Endowment*, 17(11):2750–2763.
- Tao Fan, Guoqiang Ma, Yan Kang, Hanlin Gu, Yuanfeng Song, Lixin Fan, Kai Chen, and Qiang Yang. 2025b. Fedmkt: Federated mutual knowledge transfer for large and small language models. In *Proceedings of the 31st International Conference on Computational Linguistics*, pages 243–255.
- Yijiang Fan, Yuren Mao, Longbin Lai, Ying Zhang, Zhengping Qian, and Yunjun Gao. 2025c. G-boost: Boosting private slms with general llms. *arXiv preprint arXiv:2503.10367*.
- Hainan Fang, Di Huang, Yuanbo Wen, Yunpu Zhao, Tonghui He, QiCheng Wang, Shuo Wang, Rui Zhang, and Qi Guo. 2024a. GOOD: Decoding-Time Black-Box LLM Alignment.
- Zihan Fang, Zheng Lin, Zhe Chen, Xianhao Chen, Yue Gao, and Yuguang Fang. 2024b. **Automated Federated Pipeline for Parameter-Efficient Fine-Tuning of Large Language Models**.
- Farzad Farhadzadeh, Debasmit Das, Shubhankar Borse, and Fatih Porikli. 2025. **LoRA-x: Bridging foundation models with training-free cross-model adaptation**. In *The Thirteenth International Conference on Learning Representations*.
- Sebastian Farquhar, Jannik Kossen, Lorenz Kuhn, and Yarin Gal. 2024. Detecting hallucinations in large language models using semantic entropy. *Nature*, 630(8017):625–630.
- Igor Fedorov, Kate Plawiak, Lemeng Wu, Tarek Elgamal, Naveen Suda, Eric Smith, Hongyuan Zhan, Jianfeng Chi, Yuriy Hulovatyy, Kimish Patel, and 1 others. 2024. Llama guard 3-1b-int4: Compact and efficient safeguard for human-ai conversations. *arXiv preprint arXiv:2411.17713*.
- Jiale Fu, Yuchu Jiang, Junkai Chen, Jiaming Fan, Xin Geng, and Xu Yang. 2025a. Fast large language model collaborative decoding via speculation. *arXiv preprint arXiv:2502.01662*.

- Tianyu Fu, Yi Ge, Yichen You, Enshu Liu, Zhihang Yuan, Guohao Dai, Shengen Yan, Huazhong Yang, and Yu Wang. 2025b. R2r: Efficiently navigating divergent reasoning paths with small-large model token routing. *arXiv preprint arXiv:2505.21600*.
- Yichao Fu, Rui Ge, Zelei Shao, Zhijie Deng, and Hao Zhang. 2025c. Scaling speculative decoding with lookahead reasoning. *arXiv preprint arXiv:2506.19830*.
- Ananya Gangavarapu. 2024. Enhancing guardrails for safe and secure healthcare ai. *arXiv preprint arXiv:2409.17190*.
- Luyao Gao, Jianchun Liu, Hongli Xu, Xichong Zhang, Yunming Liao, and Liusheng Huang. 2025a. Collaborative speculative inference for efficient llm inference serving. *arXiv preprint arXiv:2503.10325*.
- Shiping Gao, Fanqi Wan, Jiajian Guo, Xiaojun Quan, and Qifan Wang. 2025b. Advantage-guided distillation for preference alignment in small language models. In *The Thirteenth International Conference on Learning Representations*.
- Zhidong Gao, Yu Zhang, Zhenxiao Zhang, Yanmin Gong, and Yuanxiong Guo. 2024. FedPT: Federated Proxy-Tuning of Large Language Models on Resource-Constrained Edge Devices.
- Lovedeep Gondara, Jonathan Simkin, Shebnum Dejvi, Gregory Arbour, and Raymond Ng. 2025. Elm: Ensemble of language models for predicting tumor group from pathology reports. *arXiv preprint arXiv:2503.21800*.
- Sachin Goyal, David Lopez-Paz, and Kartik Ahuja. 2025. Distilled pretraining: A modern lens of data, in-context learning and test-time scaling. *arXiv preprint arXiv:2509.01649*.
- Yuxian Gu, Li Dong, Furu Wei, and Minlie Huang. 2024. MiniLLM: Knowledge distillation of large language models. In *The Twelfth International Conference on Learning Representations*.
- Yuxian Gu, Hao Zhou, Fandong Meng, Jie Zhou, and Minlie Huang. 2025. MiniPLM: Knowledge distillation for pre-training language models. In *The Thirteenth International Conference on Learning Representations*.
- Tom Gunter, Zirui Wang, Chong Wang, Ruoming Pang, Andy Narayanan, Aonan Zhang, Bowen Zhang, Chen Chen, Chung-Cheng Chiu, David Qiu, and 1 others. 2024. Apple intelligence foundation language models. *arXiv preprint arXiv:2407.21075*.
- Seungju Han, Kavel Rao, Allyson Ettinger, Liwei Jiang, Bill Yuchen Lin, Nathan Lambert, Yejin Choi, and Nouha Dziri. 2024. Wildguard: Open one-stop moderation tools for safety risks, jailbreaks, and refusals of llms. *Advances in Neural Information Processing Systems*, 37:8093–8131.
- Zixu Hao, Huiqiang Jiang, Shiqi Jiang, Ju Ren, and Ting Cao. 2024. Hybrid slm and llm for edge-cloud collaborative inference. In *Proceedings of the Workshop on Edge and Mobile Foundation Models*, pages 36–41.
- Florian Hartmann, Duc-Hieu Tran, Peter Kairouz, Victor Cărbune, and Blaise Aguera Y Arcas. 2024. Can LLMs get help from other LLMs without revealing private information? In *Proceedings of the Fifth Workshop on Privacy in Natural Language Processing*, pages 107–122, Bangkok, Thailand. Association for Computational Linguistics.
- Pengcheng He, Xiaodong Liu, Jianfeng Gao, and Weizhu Chen. 2021. {DEBERTA}: {DECODING}-{enhanced} {bert} {with} {disentangled} {attention}. In *International Conference on Learning Representations*.
- Yuanyang He, Zitong Huang, Xinxing Xu, Rick Siew Mong Goh, Salman Khan, Wangmeng Zuo, Yong Liu, and Chun-Mei Feng. 2024. CPT: Consistent Proxy Tuning for Black-box Optimization.
- I-Hung Hsu, Zifeng Wang, Long Le, Lesly Miculicich Werlen, Nanyun Peng, Chen-Yu Lee, and Tomas Pfister. 2024. Calm: Contrasting large and small language models to verify grounded generation. In *Findings of the Association for Computational Linguistics ACL 2024*, pages 12782–12803.
- James Y. Huang, Wenzuan Zhou, Fei Wang, Fred Morstatter, Sheng Zhang, Hoifung Poon, and Muhan Chen. 2025a. Offset unlearning for large language models. *Transactions on Machine Learning Research*.
- Kaiyu Huang, Hao Wu, Zhubo Shi, Han Zou, Minchen Yu, and Qingjiang Shi. 2025b. Specserve: Efficient and slo-aware large language model serving with adaptive speculative decoding. *arXiv preprint arXiv:2503.05096*.
- Xinyu Huang, Leming Shen, Zijing Ma, and Yuanqing Zheng. 2025c. Towards privacy-preserving and personalized smart homes via tailored small language models. *Preprint*, arXiv:2507.08878.
- Hakan Inan, Kartikeya Upasani, Jianfeng Chi, Rashi Rungta, Krithika Iyer, Yuning Mao, Michael Tontchev, Qing Hu, Brian Fuller, Davide Testuggine, and 1 others. 2023. Llama guard: Llm-based input-output safeguard for human-ai conversations. *arXiv preprint arXiv:2312.06674*.
- Daniel Israel, Guy Van den Broeck, and Aditya Grover. 2025. Accelerating diffusion llms via adaptive parallel decoding. *arXiv preprint arXiv:2506.00413*.
- Metod Jazbec, Menglin Xia, Ankur Mallick, Daniel Madrigal, Dongge Han, Samuel Kessler, and Victor Rühle. 2024. On efficient distillation from llms to slms. In *NeurIPS 2024 Workshop on Fine-Tuning in Modern Machine Learning: Principles and Scalability*.

- Dongfu Jiang, Xiang Ren, and Bill Yuchen Lin. 2023. Llm-blender: Ensembling large language models with pairwise ranking and generative fusion. In *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 14165–14178.
- Xiaoqi Jiao, Yichun Yin, Lifeng Shang, Xin Jiang, Xiao Chen, Linlin Li, Fang Wang, and Qun Liu. 2020. **TinyBERT: Distilling BERT for natural language understanding**. In *Findings of the Association for Computational Linguistics: EMNLP 2020*, pages 4163–4174, Online. Association for Computational Linguistics.
- Yizhu Jiao, Xuchao Zhang, Zhaoyang Wang, Yubo Ma, Zhun Deng, Rujia Wang, Chetan Bansal, Saravan Rajmohan, Jiawei Han, and Huaxiu Yao. 2024. **Synergistic weak-strong collaboration by aligning preferences**. In *Adaptive Foundation Models: Evolving AI for Personalized and Efficient Learning*.
- Lyudong Jin, Yanning Zhang, Yanhan Li, Shurong Wang, Howard H Yang, Jian Wu, and Meng Zhang. 2025. Moe<sup>2</sup>: Optimizing collaborative inference for edge large language models. *arXiv preprint arXiv:2501.09410*.
- Minki Kang, Jongwon Jeong, Seanie Lee, Jaewoong Cho, and Sung Ju Hwang. 2025. Distilling llm agent into small models with retrieval and code tools. *arXiv preprint arXiv:2505.17612*.
- Kyeonghyun Kim, Jinhee Jang, Juhwan Choi, Yoonji Lee, Kyohoon Jin, and YoungBin Kim. 2025. **Plug-in and fine-tuning: Bridging the gap between small language models and large language models**. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 5434–5452, Vienna, Austria. Association for Computational Linguistics.
- Sehoon Kim, Karttikeya Mangalam, Suhong Moon, Jitendra Malik, Michael W Mahoney, Amir Gholami, and Kurt Keutzer. 2023. Speculative decoding with big little decoder. *Advances in Neural Information Processing Systems*, 36:39236–39256.
- Avinash Kumar, Sujay Sanghavi, and Poulami Das. 2025. Hispec: Hierarchical speculative decoding for llms. *arXiv preprint arXiv:2510.01336*.
- Woosuk Kwon, Zhuohan Li, Siyuan Zhuang, Ying Sheng, Lianmin Zheng, Cody Hao Yu, Joseph Gonzalez, Hao Zhang, and Ion Stoica. 2023. Efficient memory management for large language model serving with pagedattention. In *Proceedings of the 29th symposium on operating systems principles*, pages 611–626.
- Yanis Labrak, Adrien Bazoge, Emmanuel Morin, Pierre-Antoine Gourraud, Mickael Rouvier, and Richard Dufour. 2024. **BioMistral: A collection of open-source pretrained large language models for medical domains**. In *Findings of the Association for Computational Linguistics: ACL 2024*, pages 5848–5864, Bangkok, Thailand. Association for Computational Linguistics.
- Jooyoung Lee, Fan Yang, Thanh Tran, Qian Hu, Emre Barut, and Kai-Wei Chang. 2024. Can small language models help large language models reason better?: Lm-guided chain-of-thought. In *Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024)*, pages 2835–2843.
- Yaniv Leviathan, Matan Kalman, and Yossi Matias. 2023. Fast inference from transformers via speculative decoding. In *International Conference on Machine Learning*, pages 19274–19286. PMLR.
- Juanhui Li, Sreyashi Nag, Hui Liu, Xianfeng Tang, Sheikh Muhammad Sarwar, Limeng Cui, Hansu Gu, Suhang Wang, Qi He, and Jiliang Tang. 2025a. **Learning with less: Knowledge distillation from large language models via unlabeled data**. In *Findings of the Association for Computational Linguistics: NAACL 2025*, pages 2627–2641, Albuquerque, New Mexico. Association for Computational Linguistics.
- Mingzhe Li, Jing Xiang, Qishen Zhang, Kaiyang Wan, and Xiuying Chen. 2025b. Flipping Knowledge Distillation: Leveraging Small Models’ Expertise to Enhance LLMs in Text Matching. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 22218–22229, Vienna, Austria. Association for Computational Linguistics.
- Senyao Li, Haozhao Wang, Wenchao Xu, Rui Zhang, Song Guo, Jingling Yuan, Xian Zhong, Tianwei Zhang, and Ruixuan Li. 2025c. Collaborative inference and learning between edge slms and cloud llms: A survey of algorithms, execution, and open challenges. *arXiv preprint arXiv:2507.16731*.
- Tianlin Li, Qian Liu, Tianyu Pang, Chao Du, Qing Guo, Yang Liu, and Min Lin. 2024a. Purifying large language models by ensembling a small language model. *arXiv preprint arXiv:2402.14845*.
- Weizhen Li, Junbao Huang, Peijie Huang, Yuhong Xu, and Jiekun Fan. 2025d. **Synergistic augmentation: Enhancing cross-domain zero-shot slot filling with small model-assisted large language models**. In *Findings of the Association for Computational Linguistics: ACL 2025*, pages 21299–21312, Vienna, Austria. Association for Computational Linguistics.
- Xiang Li, Zhenyan Lu, Dongqi Cai, Xiao Ma, and Meng-wei Xu. 2024b. Large language models on mobile devices: Measurements, analysis, and insights. In *Proceedings of the Workshop on Edge and Mobile Foundation Models*, pages 1–6.
- Xiangchen Li, Dimitrios Spatharakis, Saeid Ghafouri, Jiakun Fan, Hans Vandierendonck, Deepu John, Bo Ji, and Dimitrios Nikolopoulos. 2025e. Sled: A speculative llm decoding framework for efficient edge serving. *arXiv preprint arXiv:2506.09397*.

- Yanan Li, Fanxu Meng, Muhan Zhang, Shuai Zhu, Shangguang Wang, and Mengwei Xu. 2025f. Lorasuite: Efficient lora adaptation across large language model upgrades. *arXiv preprint arXiv:2505.13515*.
- Yuetai Li, Xiang Yue, Zhangchen Xu, Fengqing Jiang, Luyao Niu, Bill Yuchen Lin, Bhaskar Ramasubramanian, and Radha Poovendran. 2025g. Small models struggle to learn from strong reasoners. In *Findings of the Association for Computational Linguistics: ACL 2025*, pages 25366–25394, Vienna, Austria. Association for Computational Linguistics.
- Jinggui Liang, Lizi Liao, Hao Fei, and Jing Jiang. 2024. Synergizing large language models and pre-trained smaller models for conversational intent discovery. In *Findings of the Association for Computational Linguistics ACL 2024*, pages 14133–14147.
- Alisa Liu, Xiaochuang Han, Yizhong Wang, Yulia Tsvetkov, Yejin Choi, and Noah A. Smith. 2024a. Tuning language models by proxy. In *First Conference on Language Modeling*.
- Xiaoxuan Liu, Cade Daniel, Langxiang Hu, Woosuk Kwon, Zhuohan Li, Xiangxi Mo, Alvin Cheung, Zhijie Deng, Ion Stoica, and Hao Zhang. 2024b. Optimizing speculative decoding for serving large language models using goodput. *arXiv preprint arXiv:2406.14066*.
- Xiaoxuan Liu, Lanxiang Hu, Peter Bailis, Alvin Cheung, Zhijie Deng, Ion Stoica, and Hao Zhang. 2024c. Online speculative decoding. In *Proceedings of the 41st International Conference on Machine Learning*, pages 31131–31146.
- Zechun Liu, Changsheng Zhao, Forrest Iandola, Chen Lai, Yuandong Tian, Igor Fedorov, Yunyang Xiong, Ernie Chang, Yangyang Shi, Raghuraman Krishnamoorthi, and 1 others. 2024d. Mobilellm: Optimizing sub-billion parameter language models for on-device use cases. In *Forty-first International Conference on Machine Learning*.
- Zhengxiao Liu, Bowen Shen, Zheng Lin, Fali Wang, and Weiping Wang. 2023. Maximum entropy loss, the silver bullet targeting backdoor attacks in pre-trained language models. In *Findings of the Association for Computational Linguistics: ACL 2023*, pages 3850–3868.
- Zhengxiao Liu, Fali Wang, Zheng Lin, Lei Wang, and Zhiyi Yin. 2020. De-co: A two-step spelling correction model for combating adversarial typos. In *2020 IEEE intl conf on parallel & distributed processing with applications, big data & cloud computing, sustainable computing & communications, social computing & networking (ISPA/BDCloud/SocialCom/SustainCom)*, pages 554–561. IEEE Computer Society.
- Nunzio Lorè, Alireza Sepehr Ilami, and Babak Heydari. 2024. Large model strategic thinking, small model efficiency: Transferring theory of mind in large language models. *Babak, Large Model Strategic Thinking, Small Model Efficiency: Transferring Theory of Mind in Large Language Models (May 15, 2024)*.
- Zhenyan Lu, Xiang Li, Dongqi Cai, Rongjie Yi, Fangming Liu, Xiwen Zhang, Nicholas D Lane, and Mengwei Xu. 2024. Small language models: Survey, measurements, and insights. *arXiv preprint arXiv:2409.15790*.
- Renqian Luo, Lai Sun, Yingce Xia, Tao Qin, Sheng Zhang, Hoifung Poon, and Tie-Yan Liu. 2022. Biogpt: generative pre-trained transformer for biomedical text generation and mining. *Briefings in bioinformatics*, 23(6):bbac409.
- Zheqi Lv, Tianyu Zhan, Wenjie Wang, Xinyu Lin, Shengyu Zhang, Wenqiao Zhang, Jiwei Li, Kun Kuang, and Fei Wu. 2025. Collaboration of large language models and small recommendation models for device-cloud recommendation. In *Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V. 1*, pages 962–973.
- Zheqi Lv, Wenqiao Zhang, Shengyu Zhang, Kun Kuang, Feng Wang, Yongwei Wang, Zhengyu Chen, Tao Shen, Hongxia Yang, Beng Chin Ooi, and 1 others. 2023. Duet: A tuning-free device-cloud collaborative parameters generation framework for efficient device model generalization. In *Proceedings of the ACM Web Conference 2023*, pages 3077–3085.
- Xupeng Miao, Gabriele Oliaro, Zhihao Zhang, Xinhao Cheng, Zeyu Wang, Zhengxin Zhang, Rae Ying Yee Wong, Alan Zhu, Lijie Yang, Xiaoxiang Shi, and 1 others. 2024. Specinfer: Accelerating large language model serving with tree-based speculative inference and verification. In *Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 3*, pages 932–949.
- Eric Mitchell, Rafael Rafailov, Archit Sharma, Chelsea Finn, and Christopher D Manning. 2024. An emulator for fine-tuning large language models using small language models. In *The Twelfth International Conference on Learning Representations*.
- M. Mehdi Mojarradi, Lingyi Yang, Robert McCraith, and Adam Mahdi. 2024. Improving in-context learning with small language model ensembles. In *Adaptive Foundation Models: Evolving AI for Personalized and Efficient Learning*.
- Aggrey Muhebwa and Khalid K Osman. 2025. Causal distillation: Transferring structured explanations from large to compact language models. *arXiv preprint arXiv:2505.19511*.
- Manish Nagireddy, Inkit Padhi, Soumya Ghosh, and Prasanna Sattigeri. 2024. When in doubt, cascade: Towards building efficient and capable guardrails. *arXiv preprint arXiv:2407.06323*.

- Chaoyue Niu, Yucheng Ding, Junhui Lu, Zhengxiang Huang, Hang Zeng, Yutong Dai, Xuezhen Tu, Chengfei Lv, Fan Wu, and Guihai Chen. 2025. Collaborative learning of on-device small model and cloud-based large model: Advances and future directions. *arXiv preprint arXiv:2504.15300*.
- Isaac Ong, Amjad Almahairi, Vincent Wu, Wei-Lin Chiang, Tianhao Wu, Joseph E. Gonzalez, M Waleed Kadous, and Ion Stoica. 2025. **RouteLLM: Learning to route LLMs from preference data**. In *The Thirteenth International Conference on Learning Representations*.
- Aitor Ormazabal, Mikel Artetxe, and Eneko Agirre. 2023. CombLM: Adapting Black-Box Language Models through Small Fine-Tuned Models. In *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, pages 2961–2974, Singapore. Association for Computational Linguistics.
- Anthi Papadopoulou, Yunhao Yu, Pierre Lison, and Lilja Øvrelid. 2022. **Neural Text Sanitization with Explicit Measures of Privacy Risk**. In *Proceedings of the 2nd Conference of the Asia-Pacific Chapter of the Association for Computational Linguistics and the 12th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 217–229, Online only. Association for Computational Linguistics.
- Chansung Park, Juyong Jiang, Fan Wang, Sayak Paul, and Jing Tang. 2025. **LlamaDuo: LLMOps pipeline for seamless migration from service LLMs to small-scale local LLMs**. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 33194–33215, Vienna, Austria. Association for Computational Linguistics.
- Hao Peng, Xin Lv, Yushi Bai, Zijun Yao, Jiajie Zhang, Lei Hou, and Juanzi Li. 2025. **Pre-training distillation for large language models: A design space exploration**. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 3603–3618, Vienna, Austria. Association for Computational Linguistics.
- Zhaopeng Peng, Xiaoliang Fan, Yufan Chen, Zheng Wang, Shirui Pan, Chenglu Wen, Ruisheng Zhang, and Cheng Wang. 2024. **Fedptf: Federated proxy fine-tuning of foundation models**. In *Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence, IJCAI-24*, pages 4806–4814. International Joint Conferences on Artificial Intelligence Organization. Main Track.
- Quang PM Pham, Khoi TN Nguyen, Nhi H Doan, Cuong A Pham, Kentaro Inui, and Dezhen Song. 2025. **Smallplan: Leverage small language models for sequential path planning with simulation-powered, llm-guided distillation**. *arXiv preprint arXiv:2505.00831*.
- Jiaxing QI, Zhongzhi Luan, Shaohan Huang, Carol Fung, Hailong Yang, and Depei Qian. 2024. **FD-LoRA: Personalized Federated Learning of Large Language Model via Dual LoRA Tuning**.
- Ziheng Qiao, Houquan Zhou, and Zhenghua Li. 2025. **Mixture of small and large models for Chinese spelling check**. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 28298–28311, Vienna, Austria. Association for Computational Linguistics.
- Ruiyang Qin, Jun Xia, Zhenge Jia, Meng Jiang, Ahmed Abbasi, Peipei Zhou, Jingtong Hu, and Yiyu Shi. 2024. Enabling on-device large language model personalization with self-supervised data selection and synthesis. In *Proceedings of the 61st ACM/IEEE Design Automation Conference*, pages 1–6.
- Stephan Rabanser, Nathalie Rauschmayr, Achin Kulshrestha, Petra Poklukar, Wittawat Jitkrittum, Sean Augenstein, Congchao Wang, and Federico Tombari. 2025. **Gatekeeper: Improving model cascades through confidence tuning**. In *Tiny Titans: The next wave of On-Device Learning for Foundational Models (TTODLer-FM)*.
- Ankit Singh Rawat, Veeranjaneyulu Sadhanala, Afshin Rostamizadeh, Ayan Chakrabarti, Wittawat Jitkrittum, Vladimir Feinberg, Seungyeon Kim, Hrayr Harutyunyan, Nikunj Saunshi, Zachary Nado, and 1 others. 2024. A little help goes a long way: Efficient llm training by leveraging small lms. *arXiv preprint arXiv:2410.18779*.
- Mohammad Samragh, Seyed Iman Mirzadeh, Keivan Alizadeh-Vahid, Fartash Faghri, Minsik Cho, Moin Nabi, Devang Naik, and Mehrdad Farajtabar. 2024. **Scaling smart: Accelerating large language model pre-training with small model initialization**. In *Proceedings of The 4th NeurIPS Efficient Natural Language and Speech Processing Workshop*, volume 262 of *Proceedings of Machine Learning Research*, pages 1–13. PMLR.
- Victor Sanh, Lysandre Debut, Julien Chaumont, and Thomas Wolf. 2019. Distilbert, a distilled version of bert: smaller, faster, cheaper and lighter. *arXiv preprint arXiv:1910.01108*.
- Chenyang Shao, Xinyuan Hu, Yutang Lin, and Fengli Xu. 2025. **Division-of-thoughts: Harnessing hybrid language model synergy for efficient on-device agents**. In *Proceedings of the ACM on Web Conference 2025*, pages 1822–1833.
- Jianshu She, Zhuohao Li, Zhemin Huang, Qi Li, Peiran Xu, Haonan Li, and Qirong Ho. 2025. **Hawkeye: Model collaboration for efficient reasoning**. In *Second Conference on Language Modeling*.
- Yongliang Shen, Kaitao Song, Xu Tan, Dongsheng Li, Weiming Lu, and Yueting Zhuang. 2023. **Hugginggpt: Solving ai tasks with chatgpt and its friends in hugging face**. *Advances in Neural Information Processing Systems*, 36:38154–38180.

- Ruizhe Shi, Yifang Chen, Yushi Hu, Alisa Liu, Hanna Hajishirzi, Noah A Smith, and Simon S Du. 2024. Decoding-time language model alignment with multiple objectives. *Advances in Neural Information Processing Systems*, 37:48875–48920.
- Benjamin Spector and Chris Re. 2023. Accelerating llm inference with staged speculative decoding. *arXiv preprint arXiv:2308.04623*.
- Ziteng Sun, Ananda Theertha Suresh, Jae Hun Ro, Ahmad Beirami, Himanshu Jain, and Felix Yu. 2023. Spectr: Fast speculative decoding via optimal transport. *Advances in Neural Information Processing Systems*, 36:30222–30242.
- Ruslan Svirschevski, Avner May, Zhuoming Chen, Beidi Chen, Zhihao Jia, and Max Ryabinin. 2024. Specexec: massively parallel speculative decoding for interactive llm inference on consumer devices. In *Proceedings of the 38th International Conference on Neural Information Processing Systems*, pages 16342–16368.
- Jiejun Tan, Zhicheng Dou, Yutao Zhu, Peidong Guo, Kun Fang, and Ji-Rong Wen. 2024. Small models, big insights: Leveraging slim proxy models to decide when and what to retrieve for LLMs. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 4420–4436, Bangkok, Thailand. Association for Computational Linguistics.
- Liyan Tang, Philippe Laban, and Greg Durrett. 2024. Minicheck: Efficient fact-checking of llms on grounding documents. In *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing*, pages 8818–8847.
- Llama Team. 2024. Meta llama guard 2. [https://github.com/meta-llama/PurpleLlama/blob/main/Llama-Guard2/MODEL\\_CARD.md](https://github.com/meta-llama/PurpleLlama/blob/main/Llama-Guard2/MODEL_CARD.md).
- Omkar Chakradhar Thawakar, Ashmal Vayani, Salman Khan, Hisham Cholakkal, Rao Muhammad Anwer, Michael Felsberg, Timothy Baldwin, Eric P. Xing, and Fahad Shahbaz Khan. 2025. Mobillama: Towards accurate & lightweight fully transparent GPT. In *Sparsity in LLMs (SLLM): Deep Dive into Mixture of Experts, Quantization, Hardware, and Inference*.
- Yijun Tian, Yikun Han, Xiusi Chen, Wei Wang, and Nitesh V Chawla. 2025. Beyond answers: Transferring reasoning capabilities to smaller llms using multi-teacher knowledge distillation. In *Proceedings of the Eighteenth ACM International Conference on Web Search and Data Mining*, pages 251–260.
- GodsGift Uzor, Hasan Al-Qudah, Ynes Ineza, and Abdul Serwadda. 2025. Guarding your conversations: Privacy gatekeepers for secure interactions with cloud-based ai models. In *2025 19th International Conference on Semantic Computing (ICSC)*, pages 235–242. IEEE Computer Society.
- Chien Van Nguyen, Xuan Shen, Ryan Aponte, Yu Xia, Samyadeep Basu, Zhengmian Hu, Jian Chen, Mihir Parmar, Sasidhar Kunapuli, Joe Barrow, and 1 others. 2024. A survey of small language models. *arXiv preprint arXiv:2410.20011*.
- Bhoomit Vasani, Jack FitzGerald, Anjie Fang, and Sushmit Vaish. 2025. Phlora: data-free post-hoc low-rank adapter extraction from full-rank checkpoint. *arXiv preprint arXiv:2509.10971*.
- Yeshwanth Venkatesha, Souvik Kundu, and Priyadarshini Panda. 2025. Fast and cost-effective speculative edge-cloud decoding with early exits. *arXiv preprint arXiv:2505.21594*.
- Nikhil Vyas, Sham M. Kakade, and Boaz Barak. 2023. On provable copyright protection for generative models. In *Proceedings of the 40th International Conference on Machine Learning*, volume 202 of *Proceedings of Machine Learning Research*, pages 35277–35299. PMLR.
- Boxin Wang, Weixin Chen, Hengzhi Pei, Chulin Xie, Mintong Kang, Chenhui Zhang, Chejian Xu, Zidi Xiong, Ritik Dutta, Rylan Schaeffer, and 1 others. 2023a. Decodingtrust: A comprehensive assessment of trustworthiness in gpt models. *Advances in Neural Information Processing Systems*, 36:31232–31339.
- Fali Wang, Runxue Bao, Suhang Wang, Wenchao Yu, Yanchi Liu, Wei Cheng, and Haifeng Chen. 2024a. Infuserki: Enhancing large language models with knowledge graphs via infuser-guided knowledge integration. In *Findings of the Association for Computational Linguistics: EMNLP 2024*, pages 3675–3688.
- Fali Wang, Minhua Lin, Yao Ma, Hui Liu, Qi He, Xianfeng Tang, Jiliang Tang, Jian Pei, and Suhang Wang. 2025a. A survey on small language models in the era of large language models: Architecture, capabilities, and trustworthiness. In *Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V. 2*, pages 6173–6183.
- Fali Wang, Zheng Lin, Zhengxiao Liu, Mingyu Zheng, Lei Wang, and Daren Zha. 2021. Macrobert: Maximizing certified region of bert to adversarial word substitutions. In *International Conference on Database Systems for Advanced Applications*, pages 253–261. Springer.
- Fali Wang, Hui Liu, Zhenwei Dai, Jingying Zeng, Zhiwei Zhang, Zongyu Wu, Chen Luo, Zhen Li, Xianfeng Tang, Qi He, and 1 others. 2025b. Agenttts: Large language model agent for test-time compute-optimal scaling strategy in complex tasks. *arXiv preprint arXiv:2508.00890*.
- Fali Wang, Zhiwei Zhang, Xianren Zhang, Zongyu Wu, Tzuhalo Mo, Qiuhan Lu, Wanjing Wang, Rui Li, Junjie Xu, Xianfeng Tang, and 1 others. 2024b. A comprehensive survey of small language models in the era of large language models: Techniques, enhancements, applications, collaboration with llms, and trustworthiness. *ACM Transactions on Intelligent Systems and Technology*.

- Peihao Wang, Rameswar Panda, Lucas Torroba Henning, Philip Greengard, Leonid Karlinsky, Rogério Feris, David Daniel Cox, Zhangyang Wang, and Yoon Kim. 2023b. *Learning to grow pretrained models for efficient transformer training*. In *The Eleventh International Conference on Learning Representations*.
- Runqian Wang, Soumya Ghosh, David Cox, Diego Antognini, Aude Oliva, Rogerio Feris, and Leonid Karlinsky. 2024c. Trans-lora: towards data-free transferable parameter efficient finetuning. *Advances in Neural Information Processing Systems*, 37:61217–61237.
- Wenhui Wang, Furu Wei, Li Dong, Hangbo Bao, Nan Yang, and Ming Zhou. 2020. Minilm: Deep self-attention distillation for task-agnostic compression of pre-trained transformers. *Advances in neural information processing systems*, 33:5776–5788.
- Xinyuan Wang, Yanchi Liu, Wei Cheng, Xujiang Zhao, Zhengzhang Chen, Wenchao Yu, Yanjie Fu, and Haifeng Chen. 2025c. Mixllm: Dynamic routing in mixed large language models. In *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers)*, pages 10912–10922.
- Zhepeng Wang, Runxue Bao, Yawen Wu, Guodong Liu, Lei Yang, Liang Zhan, Feng Zheng, Weiwen Jiang, and Yanfu Zhang. 2024d. Self-guided knowledge-injected graph neural network for alzheimer’s diseases. In *International Conference on Medical Image Computing and Computer-Assisted Intervention*, pages 378–388. Springer.
- Ziyao Wang, Yexiao He, Zheyu Shen, Yu Li, Guoheng Sun, Myungjin Lee, and Ang Li. 2025d. Prada: Black-box llm adaptation with private data on resource-constrained devices. *Preprint*, arXiv:2503.14932.
- Ziyao Wang, Zheyu Shen, Yexiao He, Guoheng Sun, Hongyi Wang, Lingjuan Lyu, and Ang Li. 2024e. FLoRA: Federated fine-tuning large language models with heterogeneous low-rank adaptations. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*.
- Xiaofei Wen, Wenxuan Zhou, Wenjie Jacky Mo, and Muhamo Chen. 2025. ThinkGuard: Deliberative slow thinking leads to cautious guardrails. In *Findings of the Association for Computational Linguistics: ACL 2025*, pages 13698–13713, Vienna, Austria. Association for Computational Linguistics.
- Isabella C. Wiest, Marie-Elisabeth Leßmann, Fabian Wolf, Dyke Ferber, Marko Van Treeck, Jiefu Zhu, Matthias P. Ebert, Christoph Benedikt Westphalen, Martin Wermke, and Jakob Nikolas Kather. 2024. Anonymizing medical documents with local, privacy preserving large language models: The LLM-Anonymizer. Pages: 2024.06.11.24308355.
- Zongyu Wu, Minhua Lin, Zhiwei Zhang, Fali Wang, Xianren Zhang, Xiang Zhang, and Suhang Wang. 2025. Image corruption-inspired membership inference attacks against large vision-language models. *arXiv preprint arXiv:2506.12340*.
- Feifan Xia, Mingyang Liao, Yuyang Fang, Defang Li, Yantong Xie, Weikang Li, Yang Li, Deguo Xia, and Jizhou Huang. 2025. Cross-LoRA: A Data-Free LoRA Transfer Framework across Heterogeneous LLMs.
- Heming Xia, Tao Ge, Peiyi Wang, Si-Qing Chen, Furu Wei, and Zhifang Sui. 2023. Speculative decoding: Exploiting speculative execution for accelerating seq2seq generation. In *Findings of the Association for Computational Linguistics: EMNLP 2023*, pages 3909–3925.
- Yuchen Xia, Jiho Kim, Yuhan Chen, Haojie Ye, Souvik Kundu, Cong Callie Hao, and Nishil Talati. 2024. Understanding the performance and estimating the cost of llm fine-tuning. In *2024 IEEE International Symposium on Workload Characterization (IISWC)*, pages 210–223. IEEE.
- Guangxuan Xiao, Ji Lin, and Song Han. 2023. Offsite-tuning: Transfer learning without full model. *Preprint*, arXiv:2302.04870.
- Canwen Xu, Yichong Xu, Shuohang Wang, Yang Liu, Chenguang Zhu, and Julian McAuley. 2024a. Small models are valuable plug-ins for large language models. In *Findings of the Association for Computational Linguistics ACL 2024*, pages 283–294.
- Daliang Xu, Wangsong Yin, Xin Jin, Ying Zhang, Shiyun Wei, Mengwei Xu, and Xuanzhe Liu. 2023. Llmcad: Fast and scalable on-device large language model inference. *arXiv preprint arXiv:2309.04255*.
- Daliang Xu, Wangsong Yin, Hao Zhang, Xin Jin, Ying Zhang, Shiyun Wei, Mengwei Xu, and Xuanzhe Liu. 2024b. Edgellm: Fast on-device llm inference with speculative decoding. *IEEE Transactions on Mobile Computing*.
- Jiajun Xu, Zhiyuan Li, Wei Chen, Qun Wang, Xin Gao, Qi Cai, and Ziyuan Ling. 2024c. On-device language models: A comprehensive review. *arXiv preprint arXiv:2409.00088*.
- Ran Xu, Wenqi Shi, Yuchen Zhuang, Yue Yu, Joyce C Ho, Haoyu Wang, and Carl Yang. 2025. Collab-rag: Boosting retrieval-augmented generation for complex question answering via white-box and black-box llm collaboration. *arXiv preprint arXiv:2504.04915*.
- Ze Yang, Yihong Jin, and Xinhe Xu. 2025. Hades: Hardware accelerated decoding for efficient speculation in large language models. In *2025 6th International Conference on Computer Engineering and Application (ICCEA)*, pages 01–05. IEEE.

- Kazuki Yano, Sho Takase, Sosuke Kobayashi, Shun Kiyono, and Jun Suzuki. 2025. Efficient construction of model family through progressive training using model expansion. *arXiv preprint arXiv:2504.00623*.
- Kai Yao, Zhaorui Tan, Penglei Gao, Lichun Li, Kaixin Wu, Yinggui Wang, Yuan Zhao, Yixin Ji, Jianke Zhu, and Wei Wang. 2025. **GradOT: Training-free gradient-preserving offsite-tuning for large language models**. In *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 5115–5130, Vienna, Austria. Association for Computational Linguistics.
- Yifan Yao, Jinhao Duan, Kaidi Xu, Yuanfang Cai, Zhibo Sun, and Yue Zhang. 2024. A survey on large language model (llm) security and privacy: The good, the bad, and the ugly. *High-Confidence Computing*, 4(2):100211.
- Hongyi Yuan, Keming Lu, Fei Huang, Zheng Yuan, and Chang Zhou. 2024. Speculative contrastive decoding. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)*, pages 56–64.
- Murong Yue, Jie Zhao, Min Zhang, Liang Du, and Ziyu Yao. 2024. Large language model cascades with mixture of thought representations for cost-efficient reasoning. In *The Twelfth International Conference on Learning Representations*.
- Wenjun Zeng, Dana Kurniawan, Ryan Mullins, Yuchi Liu, Tamoghna Saha, Dirichi Ike-Njoku, Jindong Gu, Yiwen Song, Cai Xu, Jingjing Zhou, and 1 others. 2025. Shieldgemma 2: Robust and tractable image content moderation. *arXiv preprint arXiv:2504.01081*.
- Wenjun Zeng, Yuchi Liu, Ryan Mullins, Ludovic Peran, Joe Fernandez, Hamza Harkous, Karthik Narasimhan, Drew Proud, Piyush Kumar, Bhaktipriya Radharapu, and 1 others. 2024. Shieldgemma: Generative ai content moderation based on gemma. *arXiv preprint arXiv:2407.21772*.
- Huiyou Zhan, Xuan Zhang, Haisheng Tan, Han Tian, Dongping Yong, Junyang Zhang, and Xiang-Yang Li. 2025. Pice: A semantic-driven progressive inference system for llm serving in cloud-edge networks. *arXiv preprint arXiv:2501.09367*.
- Dan Zhang, Ziniu Hu, Sining Zhoubian, Zhengxiao Du, Kaiyu Yang, Zihan Wang, Yisong Yue, Yuxiao Dong, and Jie Tang. 2024a. Sciglm: Training scientific language models with self-reflective instruction annotation and tuning. *arXiv preprint arXiv:2401.07950*.
- Di Zhang, Wei Liu, Qian Tan, Jingdan Chen, Hang Yan, Yuliang Yan, Jiatong Li, Weiran Huang, Xiangyu Yue, Wanli Ouyang, and 1 others. 2024b. Chemllm: A chemical large language model. *arXiv preprint arXiv:2402.06852*.
- He Zhang, Jingyi Xie, Chuhao Wu, Jie Cai, ChanMin Kim, and John M Carroll. 2024c. The future of learning: Large language models through the lens of students. In *Proceedings of the 25th Annual Conference on Information Technology Education*, pages 12–18.
- Jun Zhang, Jue WANG, Huan Li, Lidan Shou, Ke Chen, Yang You, Guiming Xie, Xuejian Gong, and Kunlong Zhou. 2025a. **Train small, infer large: Memory-efficient LoRA training for large language models**. In *The Thirteenth International Conference on Learning Representations*.
- Kai Zhang, Congchao Wang, Liqian Peng, Alec Go, and Xiaozhong Liu. 2024d. Privacy-preserved llm cascade via cot-enhanced policy learning. *arXiv preprint arXiv:2410.08014*.
- Kaiyan Zhang, Jianyu Wang, Ning Ding, Biqing Qi, Ermo Hua, Xingtai Lv, and Bowen Zhou. 2024e. Fast and slow generating: An empirical study on large and small language models collaborative decoding. *arXiv preprint arXiv:2406.12295*.
- Kaiyan Zhang, Jianyu Wang, Ermo Hua, Binqing Qi, Ning Ding, and Bowen Zhou. 2024f. Cogenesis: A framework collaborating large and small language models for secure context-aware instruction following. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 4295–4312.
- Libo Zhang, Zhaoning Zhang, Baizhou Xu, Rui Li, Zhiliang Tian, Songzhu Mei, and Dongsheng Li. 2024g. Dovetail: A cpu/gpu heterogeneous speculative decoding for llm inference. *arXiv preprint arXiv:2412.18934*.
- Shaokun Zhang, Ming Yin, Jieyu Zhang, Jiale Liu, Zhiguang Han, Jingyang Zhang, Beibin Li, Chi Wang, Huazheng Wang, Yiran Chen, and Qingyun Wu. 2025b. **Which agent causes task failures and when? on automated failure attribution of LLM multi-agent systems**. In *Forty-second International Conference on Machine Learning*.
- Shaokun Zhang, Jieyu Zhang, Jiale Liu, Linxin Song, Chi Wang, Ranjay Krishna, and Qingyun Wu. 2024h. **Offline training of language model agents with functions as learnable weights**. In *Forty-first International Conference on Machine Learning*.
- Xinlu Zhang, Shiyang Li, Xianjun Yang, Chenxin Tian, Yao Qin, and Linda Ruth Petzold. 2024i. **Enhancing small medical learners with privacy-preserving contextual prompting**. In *The Twelfth International Conference on Learning Representations*.
- Yingyi Zhang, Pengyue Jia, Xianneng Li, Derong Xu, Maolin Wang, Yichao Wang, Zhaocheng Du, Hufeng Guo, Yong Liu, Ruiming Tang, and Xiangyu Zhao. 2025c. **Lsrp: A leader-subordinate retrieval framework for privacy-preserving cloud-device collaboration**. In *Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.2, KDD ’25*, page 3889–3900, New York, NY, USA. Association for Computing Machinery.

Zhiwei Zhang, Fali Wang, Xiaomin Li, Zongyu Wu, Xianfeng Tang, Hui Liu, Qi He, Wenpeng Yin, and Suhang Wang. 2025d. Catastrophic failure of llm unlearning via quantization. In *ICLR*.

Xuandong Zhao, Xianjun Yang, Tianyu Pang, Chao Du, Lei Li, Yu-Xiang Wang, and William Yang Wang. 2025. [Weak-to-strong jailbreaking on large language models](#). In *Forty-second International Conference on Machine Learning*.

Wenhao Zheng, Yixiao Chen, Weitong Zhang, Souvik Kundu, Yun Li, Zhengzhong Liu, Eric P. Xing, Hongyi Wang, and Huaxiu Yao. 2024. [CITER: Collaborative inference for efficient large language model decoding with token-level routing](#). In *Adaptive Foundation Models: Evolving AI for Personalized and Efficient Learning*.

Wei Zhong, Manasa Bharadwaj, Yixiao Wang, Nikhil Verma, Yipeng Ji, and Chul Lee. 2025. Cross-attention speculative decoding. *arXiv preprint arXiv:2505.24544*.

Bingjie Zhu, Zhixiong Chen, Liqiang Zhao, Hyundong Shin, and Arumugam Nallanathan. 2025. Efficient llm inference over heterogeneous edge networks with speculative decoding. *arXiv preprint arXiv:2510.11331*.

Yan Zhuang, Zhenzhe Zheng, Fan Wu, and Guihai Chen. 2024. Litemoe: Customizing on-device llm serving via proxy submodel tuning. In *Proceedings of the 22nd ACM Conference on Embedded Networked Sensor Systems*, pages 521–534.

Matthieu Zimmer, Milan Gritta, Gerasimos Lampouras, Haitham Bou Ammar, and Jun Wang. 2024. Mixture of attentions for speculative decoding. *arXiv preprint arXiv:2410.03804*.