

## 目录

1. 【CCF-AIR 青年基金】 Building large-capacity, low-cost, and high-performance zoned storage systems (基于软件分区抽象的 ZNS SSD 应用优化方法)	1
2. 【CCF-AIR 青年基金】 Video Origin Identification over Online Social Networks(视频来源取证技术研究)	3
3. 【CCF-AIR 青年基金】 Few-Shot Learning Based on Large-scale Pre-trained Multimodal Models (基于多模态预训练模型的小样本学习)	5
4. 【CCF-AIR 青年基金】 3D Reconstruction and Rendering Technology in E-commerce Application (基于神经辐射场的 3D 人脸 Avatar 技术)	6
5. 【CCF-AIR 青年基金】 Detection of screen recapture and its application to data loss prevention (数据防泄漏场景的屏幕翻拍翻录检测)	7
6. 【CCF-AIR 青年基金】 Collaborative scheduling and deployment mechanisms for edge-cloud applications based on low-power heterogeneous processors (基于低功耗异构处理器的边缘云应用协同部署及调度技术)	10
7. 【CCF-AIR 青年基金】 Knowledge Probing and Leveraging for Large-scale Pre-trained Models (面向大规模预训练模型的知识探测与知识利用)	11
8. 【CCF-AIR 青年基金】 TinyML: Deep Learning System on Battery-Powered Devices (TinyML: 低功耗设备上的深度学习系统)	14
9. 【CCF-AIR 青年基金】 A Hypervisor-based Seamless Multi-Tiered Memory Management Proposal for Virtual Machines (一种虚拟机无感的分层内存方案)	15
10. 【CCF-AIR 青年基金】 Service mesh performance tuning and software-hardware integration based optimization (服务网格性能调优及软硬结合优化)	16
11. 【CCF-AIR 青年基金】 Design and Implementation of Containerized 5G RAN Protocol Stack (容器化 5G RAN 协议栈设计与实现)	19
12. 【CCF-AIR 青年基金】 Research on Programmability of Host Network (virtual switch) Acceleration Scheme of Next-Generation Self-developed Network Chip (下一代自研网卡芯片主机网络 (AVS) 加速方案可编程能力研究)	21
13. 【CCF-AIR 青年基金】 Research on High Performance Satellite Communication (高性能卫星通信技术研究)	22

## 1.【CCF-AIR 青年基金】Building large-capacity, low-cost, and high-performance zoned storage systems (基于软件分区抽象的 ZNS SSD 应用优化方法)

申请链接:

<https://damo.alibaba.com/air/34c060c3812a495eb0cdddf33cb96eaf>

## 背景:

The rapid growths of data volume and data-intensive applications call for large-capacity, low-cost, and high-performance storage devices. The standard block interface has long been used and performed well in conventional storage devices, i.e., hard disk drives (HDDs). It provides an easy-to-use abstraction, i.e., a linear array of logical block addresses (LBAs) that can be read and written randomly, conforming to the media access characteristics of HDDs.

However, the block interface has increasingly become an obstacle for modern flash-based solid-state drives (SSDs). Due to higher performance, reliability, and energy efficiency, SSDs have been replacing HDDs and widely deployed in various storage systems. Flash memory must be erased in bulk before being overwritten and only allows sequential writes in an erase unit. To address the mismatch between such features and the block interface abstraction, an SSD employs a complicated firmware, called flash translation layer (FTL). Not only the hardware cost increases as significant amounts of computing, memory, and over-provisioned flash resources are required, but also software overheads are introduced and degrade the SSD performance and lifetime.

Recently, the zoned namespace (ZNS) interface, standardized by NVMe, is newly proposed for SSDs. The ZNS interface abstracts a storage device as an array of logical zones. Each zone contains contiguous LBAs that can only be written sequentially. This abstraction matches the write features of flash memory and thus can substantially simplify the FTL and reduce the hardware cost and software overheads. Furthermore, the ZNS interface promotes hardware and software co-optimizations by allowing host software to make application-aware data placement and I/O scheduling on flash memory. Overall, ZNS SSDs have emerged as a promising solution for building high-capacity, low-cost, and high-performance storage systems. How to design ZNS SSDs and apply them to current systems has become an interesting and hot research topic in both academia and industry.

One critical problem, which hinders the adoption and potentials of ZNS SSDs, originates from the fixed zone size restriction. For data reliability, the FTL usually organizes a line of flash blocks across many parallel dies/chips into a superblock or RAID stripe with parity. A superblock also becomes the unit of flash erasures and space allocation for new writes. To match the zone abstraction and flash layout, a ZNS SSD typically maps each zone to a dedicated superblock, whose size is fixed and large (e.g., a few gigabytes).

However, the hardware limit of a fixed and large zone size results in several drawbacks. Especially, ZNS SSDs from different manufactures or based on different flash models may have distinct zone sizes. First, a fixed zone size would prevent applications (which may differ in favorable zone sizes) from optimizing data placement according to their unique needs. Second, a large zone size would cause high garbage collection overheads, since host software has to relocate massive data between zones. Third, it is challenging to implement some advanced features based on ZNS SSDs, such as constructing a RAID system over ZNS SSDs with different

zone sizes, performing fine-grained data management on a ZNS SSD with a large zone size.

**目标:**

- A comprehensive analysis about the impacts of zone sizes of ZNS SSDs on the data management and performance of applications
- Effective approaches to address the zone size limitations of ZNS SSDs and the challenges of applying ZNS SSDs to current storage systems
- Publications of 1-2 papers in top-tier academic conferences and journals

**相关研究课题:**

- Flash translation layer of ZNS SSDs
- Data management based on ZNS SSDs
- Hardware and software co-designs of zoned storage systems

[返回目录](#)

## 2. 【CCF-AIR 青年基金】 Video Origin Identification over Online

### Social Networks(视频来源取证技术研究)

**申请链接:**

<https://damo.alibaba.com/air/d2f9b419ad514af9b1d2eaa996df05a8>

**背景:**

In recent years, with the upgrading of basic information technologies such as network technology, storage technology, coding technology, video content has shown a rapid development trend on the Internet, and has gradually become one of the main information transmission methods for the public. Video-related products of various lengths and forms have shown a surge. We can see that the short and medium video platforms represented by Tictok, Kuaishou, Bilibili, etc. have sprung up suddenly, with explosive growth from user volume to content volume; we can see that various online video live broadcasts are gradually becoming more and more popular among the public, and has begun to affect almost all industries; and we also can see that traditional video content such as movies and TV series has begun to be deeply Internet-based, online video has begun to compete with traditional film and television media for market share.

From the user's point of view, on the one hand, the development of software and hardware equipment, video platforms, and network technology has greatly reduced the cost of making and sharing videos, and each user can easily become a producer of video content. This has also resulted in a huge number of videos of various types

spread to almost all corners of the Internet that provide video services. On the other hand, for video content audiences, it is more and more convenient to watch videos, with high degree of freedom and immediacy of video content selection. Compared with static media content such as images and text, video can convey information more comprehensively and intuitively. Video content is also easier for the public to understand. It can be seen that video content is gradually becoming one of the main multimedia content of the Internet, and its proportion is increasing day by day, with huge potential and development space.

From the perspective of Alibaba Group, video content has already involved all aspects of our business. The big entertainment represented by Youku and Alibaba Pictures is bound to focus on video content; Taobao live broadcasts and product introduction video on Taobao make the correlation between video content and Alibaba's core e-commerce business more and more closely. It is foreseeable that a massive number of product introductions will be presented in the form of videos in the future. Moreover, in other scenarios of Alibaba Group, the proportion of video content is also increasing. It is undeniable that video content is also becoming a pivotal traffic portal in Alibaba and is becoming more and more important.

With the popular of online video content, a lot of related security issues are gradually exposed, especially when the source of video content is uploaded by normal users. For example, content security issues related to pornography, terrorism, violence, and politics; copyright issues such as piracy, plagiarism, and secondary editing; Traffic security issues such as on-hook, tampering, pseudo video streaming, etc. These new security issues have brought many new troubles to business operations and platform governance, and have also tested the Alibaba's technology accumulation in the video field, urging a new round of technology development and iteration.

However, it is difficult for us to solve all the problems mentioned above through a set of solutions. In this proposal, we focus on the security issues caused by video origin, including but not limited to piracy issue, recording and broadcasting phenomenon, tampering operation, and fake video streams involved in online video sources. We plan to develop an efficient forensics technology to identify the origin platform of user-uploaded image, and provide corresponding solutions for related business scenarios.

#### **目标:**

- Data set construction: An efficient video crawler to obtain video data from online platforms, A video data set with a large amount of online and off-line data.
- A feasible solution or method for video content analysis and feature extraction for target platforms.
- A feasible and effective video origin identification algorithm.

**相关研究课题:**

- Image Forensics/Anti-Forensics: Image origin/source identification; Image manipulation chain detection; Image/video operation trace removal.
- Multimedia Compression: Double/multiple multimedia compression detection; Multimedia compression parameter analysis.
- Video Coding: Online Social Networks
- Pattern Recognition and Artificial intelligence: Logo Recognition; Multimedia content captioning; Multimedia semantic segmentation;

[返回目录](#)

### **3. 【CCF-AIR 青年基金】 Few-Shot Learning Based on Large-scale Pre-trained Multimodal Models (基于多模态预训练模型的小样本学习)**

**申请链接:**

<https://damo.alibaba.com/air/dd9dff9b4ec346e0a5ee67941ca26b55>

**背景:**

The information in the digital world is presented in a mixed form of multimodal such as text, speech, images and videos. Multimodal translation technology will help alleviate language barriers in the globalization. Current machine translation methods based on deep neural networks often require a large amount of labeled training data which are very expensive to collect. These methods encounter various challenges in the low resource scenarios. However, most of practical applications are in the low resource scenarios.

Large-scale pre-training models that have developed rapidly in recent years, including large-scale pre-training models for single- or multi-modal for text, speech and image. They have achieved remarkable results on many low-resource tasks. Therefore, we propose to study few-shot learning based on multi-modal pre-trained models, and aim to achieve high-quality multi-modal translation in low-resource scenarios.

**目标:**

- Propose an advanced and effective few-shot learning algorithm that can use pre-trained models to perform multi-modal machine translation, and publish 2~3 CCF-A or CCF-B papers, submit 2~3 patent applications.

- A Prototype System of "Few-Shot Learning for Multimodal Pre-trained Large Models".
- Experiment reports on in-house real business data, the BLEU scores on few-shot system should not be lower than 90% of the system with labeled training data.

#### 相关研究课题:

- Few-shot learning for machine translation
- Transfer learning in low resource setting
- Multi-domal pre-training model
- Prompt learning for machine translation
- Cross-Modal alignment for speech translation
- Image transaltion based on large pre-trained model

[返回目录](#)

## 4. 【CCF-AIR 青年基金】 3D Reconstruction and Rendering

### Technology in E-commerce Application (基于神经辐射场的 3D 人脸 Avatar 技术)

#### 申请链接:

<https://damo.alibaba.com/air/12d4085aeba147808967813f39d65e52>

#### 背景:

With the diversified growth of e-commerce, live broadcasting, social networking, interactive entertainment and other scenes, the development of a new generation of interactive methods such as VR / AR has attracted much attention. In recent years, the integration of computer vision based on deep learning and traditional computer graphics has greatly promoted the development of 3D reconstruction and rendering technology. The increasing maturity of related technologies allows us to explore the next generation of e-commerce beyond traditional e-commerce.

The three elements of e-commerce scene are commodity (object), scene and human. Photorealistic reconstruction and rendering of commodity can show consumer more details in all directions and angles than traditional multimedia. Arbitrary scene reconstruction can create an experience and atmosphere more in line with the shopping scene. High quality human reconstruction, which can be driven to interact with commodity and scene, greatly improves consumers' shopping interest. The above three are combined to jointly build the integration and linkage between the virtual world and the real physical world, serve the vast e-commerce industry and

create the next generation of immersive shopping and sales experience for consumers and merchants.

#### 目标:

- An algorithm framework for high-quality reconstruction of human, commodity (object) and scene.
- A rendering engine supporting mobile real-time neural rendering.
- A set of algorithms for editing and generation, which can edit the shape and texture of objects, transform the style of scenes and enable multimodal human animation.

#### 相关研究课题:

- Fast and photorealistic head / half body / full body reconstruction from RGB video in unrestricted scene.
- High quality outdoor large-scale scene reconstruction, mass production of scene digital assets suitable for mainstream rendering engines.
- Fast and high-quality reconstruction of objects in unrestricted scene, and accurately decouple the attributes of geometry, texture, material and lighting.
- High-quality new view synthesis of object, human and scene.
- Robust object editing, face/body attribute editing, scene editing and style transfer.
- Multimodal high fidelity face reenactment, talk head generation, and human body animation.
- Explore neural rendering technology to improve the quality of rendering and realize real-time rendering.

[返回目录](#)

## 5. 【CCF-AIR 青年基金】 Detection of screen recapture and its application to data loss prevention (数据防泄漏场景的屏幕翻拍翻录检测)

#### 申请链接:

<https://damo.alibaba.com/air/4aff14b266874758a8cd132e4750bc99>

#### 背景:

Data security is bound to become a key research and development direction of all sectors of society. As far as concerned, the ability of data leakage prevention and traceability under the Internet sharing environment is still relatively weak, and data leakage has been happening all the time. "Insider" often has a variety of ways and

means to disclose high-risk data, especially unstructured data leakage such as screen recapture, screenshots and screen snapping.

从 2021 年年初开始，国家网信办、工信部、公安部等多部门对数据安全、网络信息安全等涉及到国家安全的领域陆续密集出台相关的监管措施，数据安全势必将成为社会各界的重点研究和发展方向。就目前情况来看，互联网共享环境下的数据防泄露与溯源能力依旧较为薄弱，各地数据安全问题频发。数据泄露一直在发生，“内鬼”往往有各种各样泄露高风险数据的方式方法，特别是类似录屏、截图、偷拍屏幕这类非结构化数据泄露方式。

We define unstructured data as data with irregular or incomplete data structure and no predefined data model, and this kind of data is difficult to be represented by the two-dimensional logical table of the database. It includes all forms of office documents, text, pictures, XML, HTML, various reports, images and audio / video information. Among the risk points of different types of unstructured data mentioned above, the most common scenario is to disclose high-risk content through screen recapture and snapping. Since everyone has mobile-phone, the high fidelity format of high-risk and sensitive information data can be obtained in a very short time through screenshots or screen recapture. Although some digital watermarking technologies can be used to track and trace the source of information leakage, the scanning ability of the current security infrastructure for unstructured data content is still insufficient, which may lead to some high-risk information can be transmitted externally by using image, audio and other carriers to penetrate the current protection ability of data security. Especially for the leaker photographers with special disclosure purpose, the shooting action is usually relatively secret. After the leaker shooting, it is likely to carry out a series of attacks on the image and erase the watermark marks contained in the high-risk content. Or further, the candid photographer is likely to disguise the images taken and recorded on the screen by means of image fusion and information hiding, so as to realize the behavior of secret transmission. At present, many enterprises allow arbitrary transmission and copying of photos and images, and there are obvious "security vulnerabilities" in image unstructured data.

非结构化数据是数据结构不规则或不完整，没有预定义的数据模型，不方便用数据库二维逻辑表来表现的数据。包括所有格式的办公文档、文本、图片、XML，HTML、各类报表、图像和音频/视频信息等等。尽管目前可以通过一些数字水印技术来实现对信息泄露的追踪和溯源，但是现在的安全基建对非结构化数据内容的扫描能力仍然存在不足，可能导致一些高风险信息可以利用图像、音频等载体进行对外传输，穿透目前数据安全的防护能力。特别是对于本身就带着特殊泄密目的的偷拍者，拍摄动作通常会进行得比较隐密，偷拍之后很可能对图像进行一系列的攻击，对高风险内容包含的水印标记进行抹除。或者更进一步地，偷拍者很可能通过图像融合、信息隐藏的手段将拍屏、录屏的图像进行伪装，从而实现秘密外传的行为。很多企业内部对于照片类的图像，可以任意传输和拷贝，存在明显的非结构化图像数据方面的“安全漏洞”。



Unstructured data leakage such as recapture and recording will have a very serious and bad negative impact on society, enterprises and individuals. Detection of mobile phone image/video recapture is an important topic related to data security. By studying efficient and accurate real-time detection of screen recapture data leakage, we can plug the data security loopholes in this aspect in the society to a great extent.

通过拍屏、录屏等非结构化数据泄漏行为将会对社会、企业和个人造成非常严重和恶劣的负面影响，因此针对拍屏、录屏的非结构化数据泄露检测是一项涉及数据安全的重要课题，通过研究高效准确的拍屏、录屏数据泄漏实时检测，可以有效拦截数据跨媒介传输泄漏。

### 目标:

This project proposes to conduct an in-depth research on two technical problems:

1) Efficient and accurate screen recapture detection technology. It can resist composite post-processing attacks including re-compression, cropping, scaling, multiple social media transmission and so on. 高效准确的屏幕翻拍、翻录检测技术。能够抵抗包含重压缩、裁剪、缩放、多次社交媒体传输等各种强度的复合后处理攻击。

2) Effectively combine the data content and recapture behavior to judge whether the recapture behavior is suspicious. When the recapture behavior is detected, the content of the recapture images and the behavior before and after the shooting are actively detected and analyzed through multi-modal machine learning technology and OCR technology, so as to effectively judge whether the recapture and the recapture behavior involve data leakage.

结合数据内容、拍摄行为，有效判断屏幕翻拍、翻录行为是否可疑的技术。在检测到屏幕翻拍发生的时候，通过多模态机器学习技术和 OCR 技术对翻拍内容和拍摄前后的操作行为进行主动检测和分析，有效判断翻拍、翻录行为是否涉及数据泄露。

### 相关研究课题:

- Efficient and accurate screen recapture detection 高效、准确的屏幕翻拍、翻录检测手段
- Analysis on the screen recapture behavior and leaked data content, effectively detect data leakage 结合数据内容、拍摄行为，有效检测数据泄漏的发生
- To reveal the post-processing trace in the process of screen recapture 揭示屏幕翻拍翻录过程中的后处理痕迹

[返回目录](#)

## 6. 【CCF-AIR 青年基金】 Collaborative scheduling and deployment mechanisms for edge-cloud applications based on low-power heterogeneous processors (基于低功耗异构处理器的边缘云应用协同部署及调度技术)

申请链接:

<https://damo.alibaba.com/air/73a3395fec1b408c8f614f9a061cec1f>

背景:

In recent years, with the rapid development of the mobile Internet and the Internet of Things, the total amount of computing devices and data in the world has continued to grow. However, with the rise of various novel applications such as autonomous driving, cloud gaming, live video, AR/VR, etc., the inherent weaknesses of cloud computing in terms of latency, energy consumption, and security and privacy are gradually exposed, affecting the speed of development and evolution of these new applications. Therefore, offloading computing to the edge has become a major trend and also attracts more and more researches from academy and industry.

However, various edge application services such as cloud gaming, machine learning inference, video codec, etc., requires different hardware resource (CPU, GPU, FPGA, Mobile SoC, etc.), heterogeneous hardware architectures (X86, ARM, etc.), and complex edge business advantages (network latency, throughput, cost, energy consumption, etc.). In addition, the edge applications often show a significant tidal phenomenon, resulting in a low overall hardware resource utilization rate. How to take full advantage of the idle computing resources and reduce the task execution cost while ensuring the QoS of the edge tasks has also become a valuable problem.

The above characteristics bring huge challenges to edge computing: in order to make full use of the hardware resources on the edge side, it is necessary to adapt a variety of novel scheduling and deployment mechanisms for diverse applications and heterogeneous hardware.

目标:

- Establish evaluation standards and systems for edge cloud applications on heterogeneous hardware, covering at least three types of typical applications and three types of heterogeneous hardware.
- Optimize typical edge applications (cloud games, video encoding and decoding, machine learning inference, 5G, etc.) on heterogeneous hardware such as ARM arrays and ARM servers with 30% performance improvement and 50% energy

consumption reduction.

- Build a collaborative scheduling and deployment system for edge applications on heterogeneous hardware, improve the resource utilization rate by 20%.

**相关研究课题:**

- Cloud computing
- Resource allocation
- Task scheduling
- Software-hardware codesign
- Edge-cloud collaboration

[返回目录](#)

## 7. 【CCF-AIR 青年基金】 Knowledge Probing and Leveraging for Large-scale Pre-trained Models (面向大规模预训练模型的知识探测与知识利用)

**申请链接:**

<https://damo.alibaba.com/air/e4d47dc696ca46f7bddc3030223c748d>

**背景:**

In recent years, large-scale pre-training models have opened up a new phase in artificial intelligence, such as BERT and GPT, which have set up milestones in the field of natural language processing. Large-scale pre-training models have gradually evolved from 'purely data-driven' to 'data & knowledge-driven', where knowledge learning and exploitation are key steps towards next-generation AI [1]. Recent works have begun to mine rich knowledge inherent in large-scale pre-trained models. [2] found that some linguistic knowledge, i.e., syntax, could be detected from the models; [3] detected a lot of world knowledge and common sense in the models. More interestingly, [4] took the linguistic knowledge extracted from the models further and continued to exploit it in downstream models, yielding better performance than the linguistic knowledge annotated by human experts.

In real-world applications, it is a critical challenge to transfer the knowledge learned from these pre-trained models to downstream models, especially for the tasks that strongly rely on factual knowledge and common sense, such as CommonsenseQA, KBQA, TableFact, etc. The popular approach to leverage pre-trained model is the fine-tuning paradigm: using a single dense vector representation as the interface between the pre-trained model and the downstream model, this paradigm is simple

and easy to use, but there is a risk of knowledge degradation due to the common carrier of text representation and knowledge representation through a single vector. Tackling the insufficiencies of the fine-tuning paradigm, a prompt-based approach has recently begun to be emphasized by modifying the construction (templates) of the inputs, but it still suffers from the following challenges.

(1) Templates often rely on manual design and have a strong influence on the ultimate performance, leading to weak model stability.

(2) It is difficult to design templates for complex tasks, such as semantic parsing tasks. Therefore, in both the finetune and prompt paradigms, there has been a gap in knowledge leveraging between the pre-trained model and the downstream task model.

To explore a new paradigm for fine-tuning pre-trained models, we expect to probe empirical knowledge in pre-trained models, in order to decouple the language representation from the knowledge representation and to better benefit downstream tasks.

One example we would like to share here is table semantic parsing, i.e., translating natural language questions to corresponding SQL queries. The essential problem in this task is to link natural language questions to table schemas, which is typically called schema linking. Conventionally, schema linking is implemented by ad-hoc rules. Such rules suffer from the problem of poor expressiveness and generalization. We found that schema linking knowledge extracted from large-scale pre-trained models is more reliable and robust. Dramatic improvement has been observed on downstream table semantic parsing tasks when such knowledge is explicitly employed.

近些年来，大规模预训练模型开启了人工智能领域的新篇章，比如 BERT、GPT 在自然语言处理领域中取得了里程碑式的进步。目前大规模预训练模型已经逐渐由「纯数据驱动」发展成为「数据知识双驱动」的模式，知识的学习与利用是迈向下一代人工智能之路的关键步骤 [1]。最近的一些工作开始证明大规模预训练模型中蕴含着丰富的知识，比如 [2] 等人发现可以从模型中探测出一些语言学知识，如句法等，[3] 等人发现模型中存在很多世界性知识及常识。更有趣的是，[4] 将从模型中探测出的语言学知识进一步的在下游模型中继续利用，比人类专家归纳的语言学知识有更好的表现。在真实场景的应用中，如何将这些预训练模型学到的知识向下游模型进行迁移，特别是在一些强依赖事实知识和常识的场景中，如常识问答、KBQA、TableFact 等任务，是一个关键问题。主流的预训练模型利用方式是微调（finetune）范式：利用单一的稠密向量表示作为大模型与下游模型之间的接口，这种范式简单好用，但由于通过一个向量作为文本表示及知识表示的共同载体，存在着知识损失的风险。针对微调范式的不足，近期基于 prompt（提示）的方式开始被重视，该方法通过改变输入的构造来缓解预训练模型和下游模型之间的鸿沟，但仍然面临以下挑战：

（1）模板常常依赖人工设计，且对最终结果影响很大，导致模型稳定性差；

(2) 在复杂任务上较难设计模板，比如 semantic parsing 任务中；所以，无论是 finetune 还是 prompt 范式，预训练模型和下游任务模型之间都存在知识利用的 GAP。

有没有更好的预训练模型利用机制呢？我们从语言表示与知识表示解耦的角度进行了一些尝试，比如在 semantic parsing 任务中，一个重要的过程是寻求自然语言和表格知识之间的链接关系，该过程目前只能依赖规则匹配完成。但当需要世界知识和常识才能理解的样例时，比如「北京」和「首都」，规则的方式就无能为力了，此时只能依赖额外的人工配置。我们发现即使下游模型使用预训练模型作为底座，通过 finetune 范式仍然无法解决这种问题。但当利用知识探针技术，发现可以直接从预训练模型中探测出「北京」和「首都」两个词之间存在很大的响应，这种离散的二元组关系就是预训练模型从大规模数据中归纳的、蕴含在模型的参数中的知识。我们将这种知识抽取出来后独立作为下游模型的输入，发现对下游任务的结果有大幅的提升（10%+）。结合已有的研究以及我们的初步探索，面向大规模预训练模型的知识探测与利用是一个很有前景的方向，一方面，可以通过显式的知识探测和知识利用来提升依赖复杂知识的下游任务，比如常识问答、KBQA、TableFact、VQA、摘要等，另一方面，显式探测的知识可以更好的指导大模型向小模型的知识迁移。作为研究方向，还存在以下技术挑战：

(1) 知识探测：需要设计更加准确高效的探测技术，一方面，需要探测技术切合模型结构、预训练的任务，保证探测出知识的准确性，另一方面，需要保证探测过程的效率，满足上线的要求。目前流行的探测技术都需要  $n^2$  的时间复杂度，成本很高，存在很大的优化空间；

(2) 知识流动：对于探测出的知识，需要考虑更好的方式传递到下游模型中，包括知识形态的定义（离散还是连续），知识利用的方式（是否需要额外的 adapter）等方面，有较多可深入挖掘的研究点；

(3) 知识融合：对于已经存在人类知识的任务，从模型探测出的知识需要与已有知识进行融合，人类知识和模型知识存在着一致性，同时还存在着互补性，也可能存在一定的冲突，如何平衡两种知识的关系是一个尚未探索的方向；

## Reference

- [1] 张钹, 朱军, 苏航, 迈向第三代人工智能, 中国科学 2020.
- [2] John Hewitt et al. A Structural Probe for Finding Syntax in Word Representations. NAACL 2019.
- [3] Petroni et al. Language Models as Knowledge Bases? EMNLP 2019.
- [4] Junqi Dai et al. 2021. Does Syntax Matter? A Strong Baseline for Aspect-based Sentiment Analysis with RoBERTa. EMNLP 2021.

## 目标:

- On tasks where knowledge/commonsense is desperately needed but such knowledge is not explicitly provided, such as CommonsenseQA 2.0, using large-scale pre-trained models for knowledge probing and leveraging is expected rank the first on the leaderboard with a 2% improvement over the current SOTA.
- On tasks where knowledge/commonsense is desperately needed and such knowledge is explicitly provided, such as TabFact, KBQA, etc, fusing human and

model knowledge is expected to get SOTA results on 10+ benchmarks.

- 在强依赖知识/常识但不存在外部知识的任务上，比如 CommonsenseQA 2.0，利用大规模预训练模型知识探测与利用的方式拿到榜单第一名，相对目前 SOTA 提升 2%；
- 在强依赖知识/常识同时存在外部知识的任务上，如 TabFact，KBQA 等，利用人类知识和模型知识融合的方式拿到 10+ 国际公开数据集的 SOTA 结果；

#### 相关研究课题：

- Knowledge probing of large-scale pre-trained models: how to efficiently and accurately probe empirical knowledge from large-scale pre-trained models.
- knowledge leveraging of large-scale pre-trained models: how to leverage the knowledge in large-scale pre-trained models to complete the transfer of knowledge from large models to downstream models.
- human and model knowledge fusion: how the knowledge learned by models can collaborate and complement the knowledge of human experts.

- 大规模预训练模型的知识探测研究：如何高效准确的从大规模预训练模型中探测出经验主义知识；
- 大规模预训练模型的知识利用研究：如何利用大规模预训练模型蕴含的知识，完成大模型向小模型的知识流动；
- 人类知识和模型知识融合的研究：模型学到的知识如何与人类专家的知识协同与互补；

[返回目录](#)

## 8. 【CCF-AIR 青年基金】TinyML: Deep Learning System on Battery-Powered Devices (TinyML: 低功耗设备上的深度学习系统)

申请链接：

<https://damo.alibaba.com/air/68ebf1d975d3485285c572316666089e>

背景：

Modern Smart City AI systems are empowered by various smart sensors. For example, traffic monitor sensors, snow/rain detectors, LIDAR on self-driving cars, etc. In these scenarios, we often encounter the following challenges:

- 1) Real-time data collection. The volume of the data is too large to upload to the center super-computer in real-time.

2) High requirements on the robustness and power-consumption. The system is often driven by battery. It must be able to work without external power supply for several hours.

3) Very limited memory.

In these scenarios, the conventional deep learning models cannot work well, due to their huge power consumption and memory occupation. Therefore, it is important to customize novel deep learning models for these scenarios.

**目标:**

- Innovate a new deep architecture optimized for battery-powered devices.
- Develop a deep learning pipeline for searching and training deep networks.
- Verify system performance on public benchmark datasets, including but not limited to FLOPs, power wattage, inference speed.
- Using MobileNet as baseline, achieve the same top-1 accuracies on ImageNet-1k with 30% less FLOPs.
- On MCU chip, accelerate the inference speed 20% v.s. MobileNet.
- On MCU chip, consume 20% less battery power v.s. MobileNet.
- Publish 1~2 CCF-A papers.

**相关研究课题:**

- Deep Network pruning and quantization
- Lightweight vision transformers
- Neural Architecture Search for TinyML
- Latency and power-consumption prediction for edge devices

[返回目录](#)

## 9. 【CCF-AIR 青年基金】 A Hypervisor-based Seamless Multi-Tiered Memory Management Proposal for Virtual Machines (一种虚拟机无感的分层内存方案)

**申请链接:**

<https://damo.alibaba.com/air/9d13cf602c3848da8543d7da865db83c>

**背景:**

Basically, the cloud hypervisor only passthrough the NVM - Non-Volatile Memory a.k.a. PMEM (e.g. AEP) to the virtual machines, then the cloud users are required to decide how to operate it. In order to deploy NVM, cloud users have to develop

professional skills by refactoring their codes to explicitly save hot and cold data in DRAM and NVM and managing NVM as a NUMA node based on some special features from guest OS. Since refactoring code to deploy NVM is usually unacceptable for cloud customers and managing NUMA node based on guest OS is not efficient, there is critical disadvantage on the current NVM memory management for virtual machines.

#### **目标:**

Propose a hypervisor-based scheme to manage DRAM/NVM as tiered memory, which can be seamlessly used by virtual machines.

- 1) An efficient solution to dynamically identify hot and cold memory pages for guest workloads.
- 2) A method to support page migration between hot and cold memory pages in case of passthrough devices.
- 3) A new memory controller prototype to accurately obtain information about hot and cold pages.

#### **相关研究课题:**

- Tiered memory management in host OS
- Workload model of guest OS
- Scan mechanism for hot and cold memory page
- Page migration during passthrough devices' DMA operation
- Acceleration engine for page migration

[返回目录](#)

## **10. 【CCF-AIR 青年基金】 Service mesh performance tuning and software-hardware integration based optimization (服务网格性能调优及软硬结合优化)**

#### **申请链接:**

<https://damo.alibaba.com/air/fa21146becd643c4bf67e61c6410d422>

#### **背景:**

服务网格技术发展迅速,但在实际应用中,也遇到了一些产品上共性的问题,包括性能影响和资源占用、协议的解耦式扩展支持、网络延迟等诸多问题,通过解决这些问题,将极大帮助用户提升服务网格的生产规模、稳定性、延时优化,从而促进用户业务应用在网格下的治理能力,为客户业务提供高性能、高吞吐、高灵活的服务治理与流量管控能力。



eBPF 是一项革命性的技术，起源于 Linux 内核，可以在操作系统内核中运行沙盒程序。它用于安全有效地扩展内核的功能，而无需更改内核源代码或加载内核模块。eBPF 有一个巨大的优势，eBPF 代码可以在运行时插入到现有的 Linux 内核中，类似于 Linux 内核模块，但与内核模块不同，它可以以安全和可移植的方式进行。因此 eBPF 是一项使 Linux 内核能够跟上快速发展的云原生技术栈的关键技术。

eBPF 将能够卸载越来越多的目前由代理执行的功能，以进一步减少开销和复杂性。其中，sockmap 就是一种基于 eBPF 的技术，它允许将 TCP 连接之间的数据转发过程卸载到内核中，减少了上下文切换以及用户态和内核态之间的数据拷贝操作，极大优化了 TCP 连接之间 socket 数据转发的性能。基于此技术，对于本地通信可以绕过 TCP/IP 协议栈将报文直接发给对端 socket，以此来提高性能。

在可观测性方面，bpftrace 将脚本编译为 BPF 字节码后，通过 BCC 和 eBPF 进行交互，能够追踪 TCP 细粒度的生命周期、线程阻塞、OOM 等。

In general, service mesh technology is developing rapidly, but in practical applications, it also encounters some common problems in products, including performance impact and resource occupation, decoupling extension support of custom protocols, network latency and many other problems. By solving these problems, it will greatly help users improve the production scale, stability, and latency reduction of service mesh, thereby promoting the management capabilities of user business applications under the service mesh, and providing high-performance, high-throughput, and highly flexible service management and Flow control capability.

eBPF is a revolutionary technology, originated in the Linux kernel, that can run sandbox programs in the operating system kernel. It is used to safely and efficiently extend the functionality of the kernel without changing the kernel source code or loading kernel modules. eBPF has a huge advantage, eBPF code can be plugged into an existing Linux kernel at runtime, similar to a Linux kernel module, but unlike a kernel module, it can be done in a safe and portable way. So eBPF is a key technology that enables the Linux kernel to keep up with the rapidly evolving cloud-native technology stack.

eBPF will be able to offload a growing number of functions currently performed by service mesh proxies to further reduce overhead and complexity. Among them, sockmap is a technology based on eBPF, which allows the data forwarding process between TCP connections to be offloaded to the kernel, which reduces context switching and data copy operations between user mode and kernel mode, and greatly optimizes the performance of data forwarding between sockets during TCP connections. Based on this technology, for local communication, the TCP/IP

protocol stack can be bypassed and the message can be sent directly to the peer socket to improve performance.

In terms of observability, after bpftrace compiles the script into BPF bytecode, it interacts with eBPF through BCC, and can track TCP fine-grained life cycle, thread blocking, OOM, etc.

### **目标:**

在技术上，服务网格数据面会更加深入地融合到整个云原生基础设施层，与基础网络、WASM VM、软硬件加速等技术交叉融合，结合调度控制、可观测性、零信任安全等能力，将服务网格技术作为云原生基础系统必不可少的重要一环。

将数据面代理逻辑放入系统内核层，这样在拦截处理网络请求的同时在内核实现部分的数据解析及流量治理，可以减少出入内核的次数，并可以在内核层面对数据代理使用的计算资源进行高优先级的保证。

此外，可以基于网格中服务的 QPS、协议、日志等内容、分析网格服务的具体应用类型和服务质量要求，并协调、推荐全链路上应用的网格规则，平衡单个服务质量与性能需求和网格整体性能需求。

Technically, the service mesh data plane will be more deeply integrated into the entire cloud-native infrastructure layer, cross-integrated with basic network, WASM VM, software and hardware acceleration and other technologies, combined with scheduling control, observability, zero-trust security and other capabilities, so that making service mesh technology as an essential part of cloud-native basic systems.

Put the data plane proxy logic into the system kernel layer, so that while intercepting and processing network requests, part of the data analysis and traffic management can be implemented in the kernel, which can reduce the number of times entering and exiting the kernel, and can control the computing resources used by the data proxy at the kernel level with high priority guarantee.

In addition, based on the QPS, protocols, logs and other contents of services in the mesh, the specific application types and service quality requirements can be analyzed, and mesh rules applied on the entire stack can be coordinated and recommended to balance individual service quality and performance., requirements and overall performance requirements of the mesh.

### **相关研究课题:**

- 使用 eBPF 代替 iptables 实现流量劫持，同时使用 sockmap 加速 Sidecar 代理和应用程序间的网络通信，在一定程度上降低了请求时延和资源开销。
- 使用 eBPF 增强服务网格中的可观察性:提出一种使用通过 eBPF 收集的内核数据来增强 Envoy 的方法，以快速区分应用程序和基础设施级别的问题。

- Using eBPF instead of iptables to achieve traffic hijacking, and using sockmap to speed up network communication between the sidecar proxy and the application, reduces the request latency and resource overhead to a certain extent.
- Using eBPF to Enhance Observability in a Service Mesh: a way of enhancing Envoy with kernel data gathered through eBPF to quickly distinguish application and infrastructure level problems.

[返回目录](#)

## 11. 【 CCF-AIR 青年基金 】 Design and Implementation of Containerized 5G RAN Protocol Stack (容器化 5G RAN 协议栈设计与实现)

申请链接:

<https://damo.alibaba.com/air/ffd6789e740642b298135ffd5c15c7a7>

背景:

The fifth generation (5G) mobile network is expected to provide support for various types of services and applications. As these services and applications can have different requirements in performance such as throughput, latency and reliability, they require high flexibility from the network design. However, the traditional network design based on specialized and customized hardware devices performs poorly when adapting to the varying performance requirements and incurs high deployment cost. To cope with such problem, softwarization and modularization have been widely adopted in the design and implementation of mobile network system. Softwarization allows the system to be built upon general-purpose hardware and reduces the deployment cost. Meanwhile, modularization improves the reusability and scalability of the system components, leading to better system flexibility.

Network system softwarization and modularization rely on network virtualization technology. As one of the popular virtualization methods, container technology is light-weighted and incurs low overhead, thus it makes a promising method for deploying the major component, i.e. Radio Access Network (RAN), of the 5G mobile network. Implementing virtualized 5G RAN (5G vRAN) system with containers includes dividing RAN as network functions and deploying them to general-purpose hardware devices. Compared with the other virtualization alternative, Virtual Machine (VM), container-based deployment has lower startup overhead and is easier to scale. In addition, communication between containers is generally of higher

efficiency and more capable in meeting the communication requirement of different applications. With containerized 5G RAN system, we expect the following benefits,

1. Lower deployment cost.
2. More fine-grained network resource allocation, lower operating cost.
3. Improved system scalability and better adaptability to different workload and performance requirement of various services and applications.

However, designing a containerized 5G RAN system that is of high-efficiency, reliable and adaptable to varying performance requirements still remains a challenge.

To summarize, the key design problems include:

1. Evaluation and optimization of 5G vRAN containerization overhead.
2. Efficiently splitting 5G vRAN protocol stack into network functions.
3. Designing high-performance container network for 5G vRAN system.
4. Designing an effective maintenance system for 5G vRAN.

#### 目标:

- A systematic evaluation of 5G vRAN containerization overhead and corresponding optimization design that minimizes or even eliminates the overhead.
- An effective 5G vRAN protocol stack split design that ensures the quick deployment of the 5G vRAN system and has the ability to adapt to different user requirements and scale dynamically to different workloads.
- A customized container network design for 5G vRAN system that optimizes the network overhead introduces by containerization and is capable of meeting the varying QoS requirement of different services and applications.
- A 5G vRAN maintenance system that effectively manages and maintains the physical resources, and achieves quick failure detection and recovery.

#### 相关研究课题:

- Virtualization of RAN with virtual machines
- Evaluation of fronthaul latency budget impacted by RAN virtualization
- Dynamic resource allocation in 5G cloud-RAN
- Computation resource sharing in 5G vRAN
- 5G network function slicing orchestration design and optimization
- Detection of latency anomalies in 5G RAN
- Orchestrating lightpath adaptation and flexible functional split to recover vRAN connectivity
- Utilizing Kubernetes for deploying 4G/5G core network

[返回目录](#)

## 12. 【CCF-AIR 青年基金】 Research on Programmability of Host Network (virtual switch) Acceleration Scheme of Next-Generation Self-developed Network Chip (下一代自研网卡芯片主机网络 (AVS) 加速方案可编程能力研究)

申请链接:

<https://damo.alibaba.com/air/3a5fa03e88c94ae0af4ac793b380f615>

背景:

Alibaba Cloud data center self-developed smart NICs have gone through many iterations and are leading the industry in performance, cost, power consumption, flexibility and other indicators, providing strong support for business development. In order to further consolidate the technical competitiveness of Alibaba Cloud on the host side of the data center, the self-developed smart NIC technology will continue to evolve towards higher performance, lower cost, and lower power consumption.

The host network is an important component of the self-developed network card, and its performance, delay and other indicators are the key indicators for building technical competitiveness. At the same time, the virtual switch service, as an overlay service on the data center side, has the characteristics of changing requirements and frequent iterations, which puts forward higher requirements for the flexibility of self-developed network cards. The virtual switch adopts a speed-separated acceleration architecture, placing the fast path in the hardware and the slow path in the CPU, achieving a balance between high performance and flexibility. For higher performance, lower power consumption, and lower cost, mainstream network cards in the industry are evolving toward ASICs. ASICs have a long R&D cycle, slow iterations, and high NRE costs. On this basis, how to support business flexibility is a major challenge we need to face.

At present, many flexible solutions have emerged in the field of smart NIC/DPU, such as multi-core ARM, NP, P4, GP, etc. The above solutions have their own characteristics and are applied in different scenarios. After many iterations, Alibaba Cloud's self-developed network card has accumulated a lot in terms of software and hardware integrated architecture, high performance, low latency, and flexibility, and has laid a solid foundation for subsequent technological evolution. Faced with the demand for next-generation self-developed network cards, especially how ASIC can support the rapid evolution of services, we need to answer a few questions.

First, What are the current host network requirements. What is the development situation in the next 3-5 years. Second, How to define the host network's need for flexibility. Third, What kind of flexibility can meet the business development in the

next 3-5 years. Fourth, Will the existing acceleration architecture continue to be applicable. How to optimize.

### 目标:

We hope to solve the following technical problems:

- 1.Precipitate a set of programmable capability evaluation models, which can quantitatively evaluate programmable capabilities from multiple dimensions, such as instruction set, operation cycle, performance, ease of use, and supported table item specifications;
- 2.Propose a new host network acceleration scheme, which can achieve a relatively balanced effect in terms of flexibility, performance, delay and other indicators under the background of ASIC;

Technical output: next-generation virtual switch software and hardware integrated acceleration solution and software/hardware source code (C, Verilog);

Paper & patents: Co-published 1 CCF-A communication conference paper and 1 patent.

### 相关研究课题:

Isolation Mechanisms for High-Speed Packet-Processing Pipelines

[https://www.usenix.org/system/files/nsdi22-paper-wang\\_tao.pdf](https://www.usenix.org/system/files/nsdi22-paper-wang_tao.pdf)

PANIC: A High-Performance Programmable NIC for Multi-tenant Networks

<https://www.usenix.org/conference/osdi20/presentation/lin>

[返回目录](#)

## 13. 【CCF-AIR 青年基金】 Research on High Performance Satellite

### Communication (高性能卫星通信技术研究)

#### 申请链接:

<https://damo.alibaba.com/air/1fd2002466104b49b18622a6d75bb95a>

#### 背景:

卫星通信被认为是 6G 通信技术的重要组成部分。地面终端将数据直接发送到卫星，然后卫星将数据转发至远端地面站，进而接入互联网。卫星运行在距地面上百至上万公里的高空中，有潜力提供覆盖全球的通信服务，包括海洋、湖泊、沙漠、高山等地区。

Satellite communication is considered an essential component of 6G communication techniques. Ground user terminals transmit data directly to satellites,

which then deliver data to remote ground stations for access to the Internet. Satellites work atop the ground with a distance of hundreds to tens of thousands of kilometers, and have the potential to provide communication services to global areas including oceans, lakes, deserts, mountains, etc.

近期，以 Starlink、OneWeb 为代表的低轨卫星星座蓬勃发展。相比传统的地球同步卫星，低轨卫星距地面距离更近，因此能够提供更大的网络带宽和更低的传输延时。这两项特性有助于支撑带宽敏感型应用（如高清视频传输）和延时敏感型应用（如远程通话、远程设备操作）。

Recently, Low Earth Orbit (LEO) satellite constellations such as Starlink or OneWeb are thriving. Compared with traditional Geosynchronous Equatorial Orbit (GEO) satellites, LEOs are much closer to the ground and can provide higher network bandwidth and lower transmission latency. These two features can support bandwidth-intensive applications (e.g. high-fidelity video transfer) and latency-sensitive applications (e.g. remote telephony, remote device operation).

为充分发挥低轨卫星大带宽、低延时的特性，为应用性能带来更好体验，我们需要解决两个主要问题。

To fully exploit the bandwidth and latency advantages of LEO satellites and provide good application performance, we should address two major problems.

其一，传统卫星通信基于 DVB 协议。DVB 由欧洲电信标准化组织 ETSI 制定，目前已经广泛应用于高轨卫星通信中。然而，DVB 协议中，调制解调和冗余机制要么无法调整、过于僵化，要么通过动态降低调制解调阶数、增加冗余倍数，追求低误码率。当应用在低轨卫星中时，DVB 协议可能无法适配信道的高度动态性，导致无法充分发挥低轨卫星大带宽、低延时的特性。

First, traditional satellite communication depends on the Digital Video Broadcasting (DVB) protocol defined by the European Telecommunications Standards Institute (ETSI). DVB is widely used in GEO communication. However, the modulation and coding scheme (MCS) in DVB is either fixed and unadjustable, or pursuing low Bit Error Rate (BER) by dynamically degrading the modulation order and increasing redundancy ratio. When used in LEO communication, DVB may fail to adapt to the high dynamics of the wireless channels, thus being unable to actually deliver the high bandwidth and low latency features of LEO.

其二，低轨卫星网络能够承载多种应用。不同类型的应用有不同的性能需求。在延时方面，诸如实时金融交易、远程通话等应用需要网络具备极低延时。在带宽方面，诸如高清视频传输等应用需要网络提供高带宽。多种多样的应用性能需求为卫星通信的传输层设计带来了挑战。

Second, LEO satellites can carry multiple types of applications with different performance requirements. With respect to latency, applications like real-time financial trading or remote telephony demand low network latency. On the other hand, applications like high fidelity video transfer require high network bandwidth. Diverse application performance requirements bring challenges to the transport layer design for satellite communication.

### 目标:

- An MCS scheme designed for LEO satellite communication, which can adapt to channel dynamics and fully deliver the bandwidth and latency features of LEO

- An application performance-aware transport layer, which can adjust transport algorithms and channel codec strategies according to diverse application performance requirements
- 适用于低轨卫星通信的信道调制解调及编码机制（MCS），适配低轨卫星信道的动态性，充分发挥低轨卫星大带宽、低延时特性
- 应用性能可感知的传输层技术，能够面向不同性能需求的应用，调整传输层算法和信道编码策略及参数

#### **相关研究课题：**

- Communication protocol designed for LEO satellites
- Modulation and demodulation method that can adapt to LEO dynamics
- Channel coded strategy that can adapt to LEO dynamics
- Congestion control algorithm for LEO satellite communication
- Prototype implementation based on Software-defined Radio (SDR)
- Audio/Video transmission techniques
- 面向低轨卫星的通信协议
- 适配低轨卫星动态性的调制解调方法
- 适配低轨卫星动态性的信道编码策略
- 面向低轨卫星的拥塞控制（CC）
- 软件定义无线电（SDR）实现
- 音视频传输技术

[返回目录](#)