信创云异构算力资源融合构建模式技术研究

韩娜[1] 张跃腾[2]

1. 河北电信设计咨询有限公司，河北 石家庄 050021；

2. 石家庄市宽带接入与传送网络优化技术创新中心，河北 石家庄 050021；

摘要：信创云是基于信息技术应用创新体系所构建的云计算平台，旨在实现核心技术的自主可控，对于保障国家信息安全、推动信息技术产业的自主创新与高质量发展具有重要意义。随着国产化软硬件生态的逐步完善，多元化的算力资源不断涌现，如何实现异构算力资源的统一纳管与高效协同成为关键课题。本文围绕信创环境下多类型算力资源的整合需求，探索融合资源池的构建模式，旨在为打造安全可靠、灵活高效的信创云平台提供理论支持与实践参考。

关键词：信创云；异构算力；融合构建模式

DOI：10.63887/fns.2025.1.4.11

引言

国家对于党政单位、央国企类各机构强制实行信创替代，要求到 2027 年底重点行业的央企、国企实现全部信创替代，信创技术的上下游产业链不够成熟，信创技术选型上有多种路线可供选择。本文提出了信创云异构算力资源融合构建模式，并建立基于异构信创云的跨架构资源协同管理模式，构建可信可控的智能云生态体系。

1 信创云异构算力资源融合构建面临的关键技术挑战

信创云算力资源融合构建上有很多技术难点，有资源异构性的抽象和建模难题、动态负载调度的困难和能效优化的困境、以及安全可信保障的技术难点。

针对资源异构性的抽象和建模难题，在信创云中多架构芯片共存使得算力资源难以统一管理，由于鲲鹏、海光、龙芯、飞腾等国内芯片指令集的不同，同一条任务需要多次编译适配，异构算力没有统一度量标准，调度算法无法准确匹配具体任务。硬件虚拟化也有区别，国产芯片虚拟化的扩展与 X86 VT-x 不一致，虚拟机不能跨架构迁移，迁移失败率相对较高。

动态负载调度、能效优化存在两难问题，混合业务场景下时空双重约束进一步增加调度难度，在多目标优化冲突下，实时任务需要低延迟，批量计算需要最大化吞吐量。在混合负载下，传统的调度器会出现任务超时率高、资源利用率低的情况；能耗管理不够平衡，海光服务器能耗大于同等性能的鲲鹏服务器。

安全可信保障面临着由于国产 CPU 和加速器间指令集不一致所造成的国密算法硬件加速模块难以做到通用化部署以及跨平台的数据传输效率不高且不兼容的问题。异构架构下的加速器硬件分区方式各不相同，因此难以做到统一的多租户细粒度隔离方案，并且不同的资源切片很容易产生安全边界模岸的风险[1]。

2 信创云异构算力资源融合构建的关键技术

2.1 统一抽象建模技术

在信创背景下实现异构算力资源的融合管理，首先要解决因为不同的硬件架构而导致的软硬件的不兼容问题。基于此提出分层式硬件抽象模型，在三级抽象的基础上实现国产化芯片的统一纳管。分层式硬件抽象模型主要包含驱动封装层、抽象描述层与服务接口层三个部分组成。

驱动封装层主要用于屏蔽国产芯片指令集的不同之处，通过指令转化模块完成不同的处理器架构实现其主要功能，即将物理算力资源切片并封装成虚拟化的设备，对外提供统一化、标准化的访问接口。

抽象描述层用来做硬件无关的描述，能力集规约给出计算量化的度量，拓扑关联模型是向调度器说明硬件的物理布局信息，以避免跨各个部分的性能损失。

服务接口层为上层系统提供统一注册接口以及资源查询接口两种类型的标准化接口。统一注册接口可以供国产操作系统上报设备信息。资源查询接口则允许调度器按设备类型、最小性能阈值等方式对资源进行过滤、匹配，并选择最优资源。两类接口均采用严格的接口功能原型及性能指标，达到异构资源管理服务化的功能[2]。

2.2 智能调度优化技术

基于多维建模构建优化框架，把任务执行时延以及跨架构的数据迁移延迟归入时间维度，并基于该维度进行统筹规划；同时在资源维度上跟踪资源利用率曲线、内存带宽竞争，最后基于能耗维度得到国产芯片的功耗算力关联模型。

采用近端策略优化算法优化动态决策，并结合状态空间将节点资源状态、任务需求特性及环境参数融为一类，通过其设计构建所用奖励函数包括服务质量满足率、资源均衡度以及任务功耗等指标。

通过场景化调度机制来优化性能，AI 训练任务通过拓扑感知绑定，以减少跨节点间的通信量[3]。

2.3 安全可信保障技术

从各方面加强系统安全防护，打造“三横一纵”的整体防护体系。

传输安全使用国密算法将 CPU 和加速器之间的数据流加密传输，在保证安全的同时也保证了性能上的高效率；运行隔离方面，通过采用硬件分区的方式将 NPU 算力切分为很多小的部分来满足不同的租户的使用要求；可信验证方面，采用从 BIOS 启动到容器加载全过程的度量的完整度量链机制，通过国产可信密码模块自动生成完整性报告，让整个系统的各个环节均能保证自身的可信可控性，并且是闭环式的可信验证机制[4]。

3 信创云异构算力资源融合构建模式

3.1 系统架构设计

采用分层解耦架构实现信创云异构算力融合，自底向上划分为四层逻辑结构：基础能力层、抽象服务层、调度控制层和应用接口层。

3.1.1 基础能力层

基于自主可控的异构计算平台，将基础能力层深度融合于多核 ARM 处理器、人工智能加速单元和可编程逻辑器件三种硬件形态中，其中，高算力的多核 ARM 架构处理器作为基础能力层提供通用计算能力，专用人工智能加速卡可进行混合精度计算范式的支持，并且支持硬件级的可编程逻辑器件所实现的动态重构能力，上述异构计算单元经过高带宽、低延时的 RDMA 互连网络组装形成集群部署，使用先进的网络拓扑方案保证亚微秒级的通信能力。

基于 PCIe SR-IOV 技术实现基础能力层的物理设备虚拟化，每张加速卡可以虚拟化成多个相互隔离且独享地址空间以及 DMAR 地址空间的虚拟功能单元，让虚拟机能享有类似于物理设备的操作权，大幅降低虚拟化开销。通过 RoCEv2 等标准协议实现以太网物理设备间的远程直接内存访问；并结合协议栈卸载、拥塞控制、流量调度等技术建立零拷贝的网络传输机制，实现跨节点的高带宽、微秒级时延和无损访问内存在内的各种高阶的功能特性[5]。

资源池化管理系统的层次化抽象架构中，物理资源层汇聚异构计算资源，虚拟资源层根据需求生成通用的标准计算实例或者服务实例，服务资源层封装容器化计算任务等。针对资源池化管理的安全性问题，在固件层面上实现了安全加强及密码算法加速，并且结合硬件辅助开发虚拟化功能的热迁移技术，优化了跨子网远程内存访问路径，并基于异构硬件构建了面向异构硬件的任务调度策略。

3.1.2 抽象服务层

抽象服务层是异构计算资源的统一纳管枢纽，以硬件无关的描述模型作为跨架构芯片之间的统一硬件适配层。采用声明式描述语言确定计算资源的通用属性，包括指令集特征、计算能力维度和安全策略维度，并制定元数据目录结构规范。当有新的国产化处理器上线时，基于硬件特征指纹按照指令集架构变体动态注册，自动生成标块化设备描述符，并对其进行如下属性的要素描述：第一类是算力特征集，用来标识处

理器可以支持什么类型的并行计算范式以及是否有附加的特定类型指令的扩展；第二类是拓扑位置信息，是对物理设备映射到计算集群后的逻辑拓扑位置关系描述；第三类是安全属性域，用于封装可信执行环境的参数和密码加速能力相关的认证信息。

通过构建抽象层来建立虚拟映射表，从而实现物理资源到逻辑空间的转变，其中映射表包含两层寻址结构，第一层为地址空间，其可以绑定唯一的描述符给物理设备；第二层地址空间对应生成脱离硬件的逻辑算力单元标识符，利用实时同步的映射引擎，异构芯片上物理资源被动态映射成具有统一接口的逻辑算力单元，不同的逻辑单元为上层算法提供了标准化的计算服务访问入口，将硬件底层差异完全屏蔽。

资源抽象网关是利用描述符转换服务将上层应用所发起的通算请求动态编译成目标硬件的原生指令序列；拓扑感知调度器根据描述符的位置信息动态调度任务给对应的物理节点，以降低任务分布过程中的跨节点通信开销；安全隔离执行环境根据描述符的安全属性建立相应的可信计算域，并且仅允许敏感的计算任务在得到硬件的保护之后才进行执行。

3.1.3 调度控制层

将调度控制层设置成调度管控层，并运用多目标深度强化学习调度器为调度控制层的核心决策引擎。对采集的基础设施层和抽象服务层状态信息进行整合，产生合适的调度策略，针对拓扑感知绑定、实时任务抢占等手段分配算力资源及保证服务质量。

调度控制层是异构计算平台的神经中枢，将基于多目标深度强化学习设计的智能调度器部署于其中，基于多元状态观测空间，收集基础设施层和抽象服务层的相关信息，形成全局资源态势图谱；将时空特征提取网络接收的动态信息流进行加工处理并最终生成相应的调度策略。

调度执行系统用协同的方式落实策略，首先实现拓扑感知的资源绑定策略，通过对设备描述符的位置信息判断出每个任务的计算任务，并把它分配给网络通信开销最小的逻辑算力单元中，以减少跨节点的数据传输时间延迟。其次实现基于实时任务抢占的调度器，优先级驱动资源重分配，使得系统能够保证关键业务流的服务质量。利用检查点保存和恢复来保证任务的连续运行。构建弹性资源伸缩通道，根据系统负载情况实时调整系统的逻辑算力单元规模。

3.1.4 应用接口层

应用接口层作为异构计算平台的服务接入层，基于标准化接口提供了一个统一的服务访问面，并且采用声明式的接口规范，同时面向 REST 风格提供应用编程接口。其中虚拟机实例化、容器化工作负载采用二态融合部署方式。另外，接口语义定义能够向后兼容所有主流的云基础设施管理标准，因此对通用的跨平台操作命令也可实现无损转换。通过工作负载描述模板库，可以将异构计算资源请求转为与平台层无关的服务定义语言表达式，使得上层应用不用关心物理硬件的类型就可以对整个计算任务进行编排。

该层充分结合国家商用密码算法模块，实现对安全传输体系的构筑；利用双因素认证实现接口访问控制，以属性为基础的动态令牌授权策略保证指令的完整性和不可抵赖性；对于数据传输采用分层加密的方式，即控制平面对指令采用轻量级密码算法，实现传输实时性要求，对于数据平面中的载荷则采用强度大的密码算法进行保护。安全审计子系统对接口调用的行为进行实时审计，通过异常流量模式识别和操作序列分析，达到国家信息系统等级安全保护的基本要求。

3.2 核心模块实现

通过资源纳管、调度决策、安全执行三个部分联动完成信创云异构算力的融合纳管。

资源纳管模块设计自动化设备探测框架，基于系统总线协议解析识别异构计算单元，利用指令集架构特征进行国产化设备硬件指纹精准匹配，并采用统一的能力上报方式，定义计算通量基准、内存访问特性、安全扩展支持等多个维度的标准元模型。嵌入式采集代理利用性能监控单元获得硬件的原始指标，进行静态规范符合性和动态微基准测试双重检验，并生成结构化设备描述文件，把能力参数集、运行约束、兼容性声明等重要的元数据进行封装。监测代理不断采集处理器的热状态参数、内存的完整性的告警信号、总线稳定性的告警信号等数据，利用时序异常检测算法对其可能存在的隐患进行捕捉并加以研判，并将准故

障发送给健康评估引擎，同时向运维管理系统提供对应的管理数据源，当到达基础阈值告警时触发日志记录，当达到趋势偏离阈值告警则开启诊断分析模式，若故障预测结果触发设备退化特性的预警阈值，则对设备进行主动的维护修复措施，当设备在状态监测模块下出现临界异常状态时，热迁移控制器根据设备描述安全隔离的信息，主动选取兼容性较好的节点进行虚拟机迁移，保证关键业务的连续性。

调用决策模块建立数据驱动的智能调度器，通过两阶段协同方式对资源池不同类资源进行分配优化。离线策略生成阶段基于系统的历史负载特征时序数据，通过近端策略优化模型训练集学习的任务资源需求模型来完成任务的初始资源分配策略的生成工作，利用深度神经网络完成任务资源需求模型到集群状态空间映射，并通过对抗性奖励塑造方法完成多目标优化。在线决策阶段将轻量化推理引擎推入系统，结合实时的基础设施层资源状态流和任务请求队列流，在不影响实时决策精度的要求下通过特征空间压缩以及决策树剪枝的方法大大降低推理延迟时间，实现针对特定业务节点级别的调度指令的毫秒级响应。最后输出计算单元绑定策略、优先级分配方案和资源预留指令。

构建的安全执行模块从硬件信任根出发，以国密算法体系为基础，对密钥全生命周期进行管理。密钥管理层利用物理不可克隆技术和安全熔断技术来确保密钥从生成到销毁的全过程具有可验证性。计算保护层把敏感数据的解密和密态计算交由硬件加速器安全分区执行，规避该过程遭受时序分析和功耗分析等侧信道攻击。审计追溯层部署轻量级分布式账本框架，把算力访问的操作轨迹全部记录下来，利用国密算法给审计事件打上时间戳，防止上述行为不能被抵赖且完整无误，符合信息系统安全等级保护中关于审计追踪的相关要求。

资源纳管、调度决策、安全执行三大模块通过轻量化设计和解耦合架构，在保障系统安全合规的同时，做到高效运转。

结语

本文探索了信创云环境下异构算力资源的融合构建模式。通过建立分层式硬件抽象模型，旨在解决国产多架构芯片的统一纳管难题；创新设计的智能调度优化框架可实现多维资源协同管理，显著提升算力利用效能；构建安全可信执行体系，以全面满足等保合规要求。通过构建融合模式，在保障安全可控的前提下，优化跨架构算力协同效率，为信创云平台建设提供切实可行的技术路径。

参考文献

[1] 国家工业信息安全发展研究中心信息技术应用创新产业发展报告（2023）[R].北京：电子工业出版社，2023.

[2] 张立华，李庆华.云环境异构计算资源自适应调度模型研究[J].计算机学报，2023，46(5)：1021-1035.

[3] 王建军，陈志强，刘洋.基于国密算法的云数据安全传输架构[J]. 软件学报，2022，33(8)：2987-3002.

[4] 刘伟，张晓东. 信创云平台架构设计及关键技术研究[J]. 计算机工程与设计，2023，44(10)：2785－2791.

[5] 王磊，陈立平. 基于国产软硬件生态的信创云实践探索[J]. 信息网络安全，2023(6)：75－81.