基于访问权限控制博弈的容器安全隔离机制研究

温佳坤[1,2]，曹源[1]，孙永奎[1]，王峰[1]，邱兆阳[2]
（1.北京交通大学自动化与智能学院，北京 100044；2.北京全路通信信号研究设计院集团有限公司，北京 100070）

摘　要：为实现高铁列车客运服务边缘计算资源的安全隔离，首先，建立了基于云边端协同架构的客运服务系统业务场景下的权限控制博弈模型。在传统基于属性的访问控制（ABAC）基础上动态控制客体容器的访问权限，以最大限度地降低容器逃逸对宿主机及其他共享资源容器的影响。然后，将博弈理论引入容器权限动态调整中，设计基于奖惩机制的访问权限控制博弈约束机制，以权限激励驱动，奖励受控容器，惩罚有逃逸倾向的容器，实现基于权限控制实现处理能力与安全隔离的总体均衡。最后，通过仿真分析证明，基于奖惩机制的访问权限控制博弈约束机制可以有效提升容器的安全隔离性能，有效降低逃逸风险，且不会对宿主机带来过度负载。

关键词：云边端协同；容器；安全隔离；权限动态调整；博弈理论
中图分类号：U28
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025188

Research on container security isolation mechanism based on access permission control game

WEN Jiakun[1,2], CAO Yuan[1], SUN Yongkui[1], WANG Feng[1], QIU Zhaoyang[2]
1. School of Automation and Intelligence, Beijing Jiaotong University, Beijing 100044, China
2. CRSC Research & Design Institute Group Co., Ltd., Beijing 100070, China

Abstract: To achieve the secure isolation of edge computing resources for passenger transportation services on high-speed trains, a permission control game model in the business scenarios of the passenger transportation service system based on the cloud-edge-end collaborative architecture was first established. Based on the traditional attribute-based access control (ABAC), the access rights of object containers were dynamically controlled to minimize the impact of container escape on the host machine and other containers sharing resources. Then, the game theory was introduced into the dynamic adjustment of container permissions, and a game constraint mechanism for access permission control based on a reward and punishment mechanism was designed. Driven by permission incentives, controlled containers were rewarded, and containers with an escape tendency were punished, so as to achieve the overall balance between processing power and secure isolation through permission control. Finally, simulation analysis proves that the game constraint mechanism for access permission control based on the reward and punishment mechanism can effectively enhance the secure isolation performance of containers, effectively prevent the escape risk, and will not impose excessive load on the host machine.

Keywords: cloud-edge-end collaboration, container, secure isolation, dynamic adjustment of permission, game theory

收稿日期：2025–05–28；**修回日期：**2025–08–12
通信作者：温佳坤，23115037@bjtu.edu.cn
基金项目：国家自然科学基金资助项目（No.U2368202, No.U2468203）
Foundation Items：The National Natural Science Foundation of China (No.U2368202, No.U2468203)

0 引言

近年来，我国高速铁路迅猛发展，经过十几年大规模的高铁建设，无论是在运行速度上，还是在运营里程上都已处于世界前列[1-2]。高铁的快速发展对高铁客运服务水平和安全保障能力也提出了更高的要求[3]。尽管现有的列车客运管理信息系统为高铁客运服务提供了重要支撑，但随着高铁列车客运服务的多样化，如车载计算资源不足难以应对大量数据和业务的处理任务、隐私泄露风险大难以保证旅客信息安全、客运服务管理信息各子系统之间信息壁垒高筑、高效安全的协同服务难以形成等现有系统性能和客运服务质量提升需求之间的矛盾日益凸显。边缘计算的分布式架构、靠近终端和低时延响应能力为解决列车客运服务中车载终端算力不足的问题提供了可能。同时云边融合的资源协同架构也为打破客运服务信息壁垒，实现列车客运服务管理技术变革提供了新的解决方案[4]。然而，高铁列车具有高速移动特征、客运服务业务涉及数据隐私性等特点，故构建适合于高铁列车客运服务的云边端协同管理信息系统面临诸多挑战。

高铁列车行车密度高、车上客运业务繁忙等特点使列车客运服务在边缘侧的业务处理需求急剧增长，呈现显著的高并发特征[5]。此外，列车行驶速度高，对边缘计算的处理和响应速度也有着极高的要求，其实现基础是地面分布式资源的高效管理和利用，核心在于资源虚拟化管理。然而资源虚拟化本质是以共享为基础的资源抽象化，必然涉及边缘资源、数据和应用的安全隔离问题。因此，如何在提升边缘资源管理效率的同时实现安全隔离是列车客运服务管理信息系统所面临的重要挑战。

容器虚拟化技术在轻量化和可移植性方面有着优良的特性，其安全性也不容忽视。李佳曦[6]将容器虚拟化技术引入以规避云平台的内核安全风险、镜像安全风险、主机安全风险和网络安全风险，提升了虚拟化过程的安全性。Jiang等[7]针对Docker漏洞提出了避免文件之间的交互、基于PID命名空间分隔进程域名和主机名的隔离及隔离网络资源4个方面的解决方案。Zerouali等[8]研究了社区镜像中JavaScript、Python和Ruby包过时程度和漏洞，表明Docker Hub社区镜像中漏洞数量较多，需投入更多维护或在应用时进行安全防护。Liu等[9]提出了Docker镜像的主要安全风险源，包括敏感参数、恶意程序和未修补的软件漏洞。此外，容器逃逸和拒绝服务（DoS, denial of service）攻击也是容器虚拟化技术的重要风险所在。张云涛等[10]提出了一种基于特征提取的实时容器逃逸检测方法，提高了容器逃逸的准确率。胥柯等[11]提出了使用CFMAC模型对Docker容器管理程序进行加固，并通过3个等级的安全校验，有效降低了Docker容器逃逸带来的危害。王杰等[12]设计了基于Docker容器行为分析的安全隔离系统架构，结合人工智能方法实现服务过程中异常的及时检测。针对分布式拒绝服务攻击检测难题，陈红松等[13]模拟了4种不同的流量攻击模式，在此基础上提出了一种流量异常检测方法。季一木等[14]提出了一种基于调用频率的入侵检测方法，实现了容器拒绝服务攻击的检测。

Bui[15]揭示了通过命名空间和cgroup实现的默认安全配置具备基本隔离有效性，但其结论基于理想化假设的测试环境，未能充分考虑实际生产环境中多租户场景下的复杂交互风险。该研究提出的最小特权原则在实际应用中常因遗留系统兼容性需求而难以彻底实施，且未量化分析特权残留可能造成的攻击面扩展问题。针对安全增强机制的研究中，文献[16-17]提出的SELinux配置文件扩展方案虽解决了多容器同类型标签的安全缺陷，但其方法论存在显著局限性。首先，要求开发者具备SELinux策略编写能力，这与DevOps实践中开发人员的安全技能水平存在现实差距。其次，静态策略绑定机制难以适应动态编排环境下的容器生命周期管理需求，可能引发策略与运行环境的不匹配风险。Miller等[18]提出的通用安全评估模型虽为跨平台比较提供了理论基础，但其评估维度偏重架构设计层面的形式化分析，缺乏对实时攻击场景的动态验证，特别是对零日漏洞的防御能力评估存在空白。在攻击检测与防御技术层面，Jian等[19]提出的命名空间状态监测方法虽能有效识别异常进程，但其基于运行时监控的机制会引入约7%~15%的性能损耗（根据原始实验数据），这对时延敏感型应用构成实质性部署障碍。同时，该方法对内核级逃逸攻击的检测存在盲区，无法覆盖通过未初始化命名空间进行的隐蔽攻击。Chelladhurai等[20]提出的内存限制技术虽能缓解DoS攻击，但其防御效果高度依赖预设阈值，缺乏自适应资源调控机制，在突发流量场景下可能造成误阻断。该技术对新型内存耗尽型攻

击（如CVE-2021-41091描述的cgroup v2漏洞）也缺乏防护能力。镜像安全领域的研究暴露出更显著的系统性缺陷。Abidrabbu等[21]对Docker Hub的漏洞分析虽揭示出严重安全隐患，但其研究方法存在三方面不足：一是基于CVE数据库的静态扫描未能评估漏洞在容器虚拟化环境中的实际可利用性；二是未建立漏洞修复时效性评估模型，无法反映社区响应速度对风险消减的影响；三是对非官方镜像供应链的污染风险缺乏溯源分析。Lu等[22]提出的渗透测试框架虽覆盖主流攻击向量，但其测试用例库更新滞后于容器虚拟化技术的快速迭代，对基于Kubernetes编排层的新型攻击路径（如sidecar注入攻击）缺乏检测能力。综合现有文献可见，Mouat[23]提出的安全建议虽具有实践价值，但其防御策略呈现碎片化特征，未能构建体系化的纵深防御模型。现有研究普遍存在“重检测轻预防、重单点轻体系”的倾向，在容器全生命周期安全管理、跨层安全策略协同、云原生威胁情报共享等关键领域仍存在显著研究空白。此外，多数安全方案与CI/CD管道的集成度不足，难以实现安全左移的现代DevSecOps要求，这已成为制约容器安全实践效果的重要瓶颈。

上文从多个角度对容器和宿主机的安全性进行了研究，并对其中存在的问题提出了各种解决方法和改进意见。但是对于镜像和共享存储这些容器自身的内容却有所忽略。这些存在于容器内部的文件也可能会遭受篡改和破坏，黑客也可能通过破坏容器自身来损害主机。

作为轻量级虚拟化的方案，容器在灵活性和可迁移性等方面有着无可替代的优势，然而由于共享宿主机内核的特征，边缘容器方案依然存在系统漏洞和安全隐患。首先，内核级漏洞的利用可能引发容器逃逸攻击，攻击者可突破隔离边界直接威胁宿主机的安全，这对要求毫秒级响应的高速票务核验、实时调度等关键业务构成严重威胁。其次，容器间共享的运行环境大幅扩展了攻击面，零日漏洞的暴露可能导致多容器横向渗透，危及车载旅客信息系统与站台协同控制模块间的数据交互安全。更严峻的是，现有基于命名空间和cgroups实现的隔离机制存在防护粒度不足的缺陷，恶意进程可能通过共享文件系统或未受控的进程间通信（IPC, interprocess communication）通道窃取旅客隐私数据或干扰应急通信服务，高速移动开放网络环境下风险加剧。同时，传统安全加固方案与实时业务需求存在矛盾，过度隔离可能造成车载传感器数据流延迟，而降低防护强度又将导致DoS攻击风险呈指数级上升。这种安全性与实时性的双重挑战，使其在保障350 km/h运行环境下毫秒级业务连续性的同时，实现细粒度计算资源隔离成为亟待攻克的技术难题。

本文主要研究如下。

1) 建立了基于云边端协同架构的客运服务系统业务场景下的权限控制博弈模型。在传统基于属性的访问控制（ABAC, attribute-based access control）基础上动态控制客体容器的访问权限，以最大限度地降低容器逃逸对宿主机及其他共享资源容器的影响。

2) 设计了基于奖惩机制的访问权限控制博弈约束机制，以权限激励驱动，奖励受控容器，惩罚有逃逸倾向的容器，实现基于权限控制实现处理能力与安全隔离的总体均衡。

3) 仿真结果表明，本文机制具有很好的容器安全隔离效果，并在最大程度上保证了容器的处理能力。与传统基于角色的访问控制策略对比，验证了本文机制的有效性。

1　云边端协同的客运服务管理系统架构

与传统云中心计算架构不同，面向客运服务的云边端协同架构中边缘计算主要负责车载终端设备海量上传数据的实时分析和处理，将处理结果返回车载终端的同时，在边缘层存储有价值的数据或上传数据至云端。云计算负责对实时性要求低、处理周期较长的数据进行存储和分析[24]。面向高铁列车客运服务的云边端协同架构如图1所示，该架构包括终端、边缘云和中心云3层。

1) 终端。主要包含车载终端和客运站段移动终端，在客运服务过程中由终端层收集乘务日志、列车速报、客运记录、应急监控及客运服务等信息，通过高铁线路附近的基站或5G网络上传至边缘层，该过程依赖开放的无线网络传输，是云边端客运服务系统中主要的信息安全风险点。

2) 边缘云。高铁客运服务过程靠近车载终端的路局和站段级平台具有强大的计算、网络、存储等能力，可以对车载终端上传的数据和任务进行处

理和存储，降低响应时延和带宽成本、减轻云端压力。受高铁线路网广而分散特征的影响，边缘层呈现天然的分布特征。将跨地域、跨系统的算力集群进行统一纳管，依赖容器虚拟化技术在有限边缘资源情况下，灵活快捷地处理实时性要求较强的计算任务和中心层传输的高强度计算数据。

3) 中心云。该层主要由铁路总公司的中心服务资源构成，是云边端协同架构中算力最强大的一级，统筹管理从边缘节点上传的信息，以及调度命令管理、在途监控、客票管理等信息，实现全路网站段、列车客运相关业务编排和处理，并对网络、算力、应用等资源进行统一管理，实现边缘系统的算法部署和运维升级，提升云边协同效率。中心层和边缘层之间采用铁路专用网络通信。

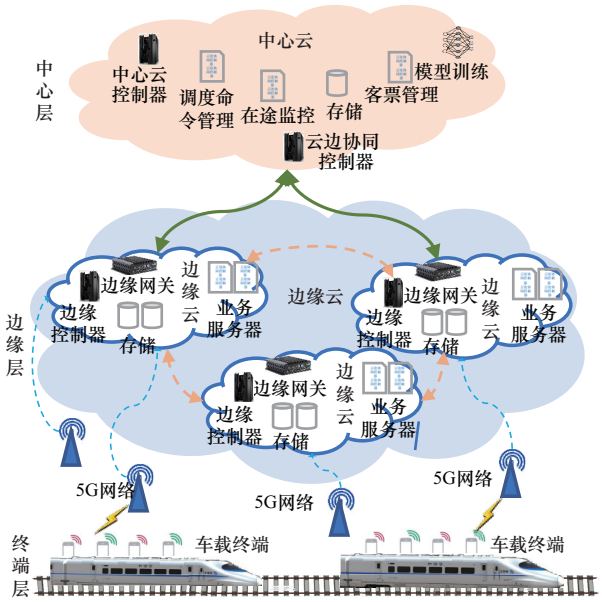


图1　面向高铁列车客运服务的云边端协同架构

在面向高铁列车客运服务的云边端协同架构基础上，建立云边端之间的协同能力，主要包括数据协同、资源协同、算法协同和应用协同4个方面。在数据协同方面，边缘节点接收车载终端设备实时产生的海量数据，并同步对数据进行处理和分析，保证应用和业务需求的实时性。在资源协同方面，边缘节点接收车载终端采集的数据，调用中心层云平台计算资源协同处理相关数据，实现三层资源的合理分配和充分利用。在算法协同方面，利用边缘集群和微服务优势，基于元学习、深度学习和联邦学习等方法，进一步感知客运过程的乘客需求，学习服务模式并综合评价客运服务质量。在应用协同方面，边缘集群提供应用的部署与运行环境，并支持云端全局控制中心对应用的自动调度和全生命周期管理。在云边端交互和多方面协同机制下，提升列车客运服务质量。但在开放网络环境下，列车的高速移动计算任务的频繁迁移，使容器访问共享文件频率增加，容器暴露风险变大，从而增加了容器逃逸的安全风险，因此需设计相应的防护机制保证系统在容器逃逸等信息安全风险下，能够正常运行。

2　容器权限控制博弈模型

容器权限控制博弈模型相关符号定义如表1所示。

表1　　相关符号定义

符号	含义
u	容器的收益函数
u	宿主机的收益函数
S	容器的策略集合
S	宿主机的策略集合
ρ	宿主机认为容器权限高的概率
θ	最低权限阈值
p	受控访问概率
φ	奖励因子
R_{ho}	容器受控访问的预期收益
U	累积收益

为提高容器安全隔离和完成既定任务的效率，本文将博弈模型应用于容器访问宿主机共享文件的权限调整过程。在客运服务的云边端协同架构下，边缘层和中心层大量使用容器承担相应的计算任务，在开放网络环境下，容器为访问宿主机的主体，宿主机作为访问的客体，在容器信息不完全透明的条件下，访问客体宿主机利用既有权限设置对访问主体容器进行判断的行为，符合不完全信息的贝叶斯动态博弈模型[25]。因此，可通过建立容器权限控制博弈模型 $G(N, \theta, S, P, U)$来描述宿主机对容器访问权限的动态调整过程，根据海萨尼（Harsanyi）转换基本思想[26]，可得访问权限控制博弈树如图2所示，参数定义如下。

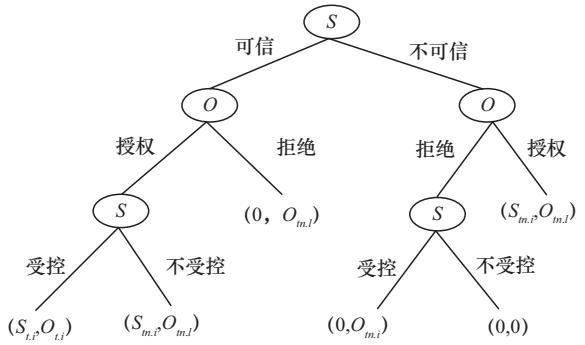


图2　访问权限控制博弈树

1) $N=\{S,O\}$是参加文件访问博弈的弈者集合，即参与访问权限交互的访问主体容器和访问客体宿主机。

2) $\theta=\theta_s\times\theta_o$，$\theta$是博弈的类型集合。

3) $S=S_s\times S_o$，S是博弈行动中所包含的策略集合，其中$S_s=\{S_s, i\in N\}$是访问主体容器的策略集合，$S_o=\{S_o, i\in N\}$是访问客体宿主机的策略集合。

4) P: $\theta\rightarrow[0,1]$, $\rho\in P$，P是客体宿主机对访问主体容器权限等级的判断，$P=\{\rho,1-\rho\}$，ρ表示客体宿主机认为访问主体容器权限高的概率，$1-\rho$表示客体宿主机认为访问主体容器权限低的概率。

5) $U=\{u_s, u_o\}$，u_s: $\theta\times S\rightarrow R$，表示访问主体容器的收益函数，$R$是收益值；$u_o$: $\theta\times S\rightarrow R$，表示访问客体宿主机的收益函数。$u_s$和$u_o$支付矩阵如表2所示。

表2　支付矩阵

博弈者		客体宿主机	
	行动	允许	拒绝
主体容器	可信受控	$S_{t.i}$, $O_{t.i}$	0, $O_{tm.i}$
	可信不受控	$S_{tm.i}$, $O_{tm.i}$	0, $O_{tm.i}$
	不可信受控	$S_{t.l}$, $O_{t.l}$	0, $O_{tm.l}$
	不可信不受控	$S_{t.l}$, $O_{t.l}$	0, 0

从表2可得出以下结论。

1) 根据访问主体容器的访问请求，在对主体容器权限高于申请访问文件安全等级且主体权限高于客体权限的情况下，客体选择授权并允许主体读写指定文件。此时，若客体权限高于被访问文件，则客体判定为受控，主客体在此次访问中的收益为($S_{t.i}$, $O_{t.i}$)。

2) 根据访问主体容器的访问请求，在对主体容器权限高于申请访问文件安全等级且主体权限高于客体权限的情况下，客体选择授权并允许主体读写指定文件。此时，若客体权限低于被访问文件，则客体判定为不受控，主客体在此次访问中的收益为($S_{tm.i}$, $O_{tm.i}$)。

3) 根据访问主体容器的访问请求，在对主体容器权限高于申请访问文件安全等级但主体权限低于客体权限的情况下，客体选择授权并拒绝主体读写指定文件，主客体收益为(0, $O_{tm.i}$)。

4) 根据访问主体容器的访问请求，在对主体容器权限低于申请访问文件安全等级但主体权限高于客体权限的情况下，客体选择授权并允许主体读写指定文件。此时，主客体收益为($S_{tm.l}$, $O_{t.l}$)。

5) 根据访问主体容器的访问请求，在对主体容器权限低于申请访问文件安全等级且主体权限低于客体权限的情况下，客体选择拒绝主体读写指定文件。此时，若客体权限高于被访问文件，则客体判定为受控，主客体收益为(0, $O_{tm.l}$)。

6) 根据访问主体容器的访问请求，在对主体容器权限低于申请访问文件安全等级且主体权限低于客体权限的情况下，客体选择拒绝主体读写指定文件。此时，若客体权限低于被访问文件，则客体判定为不受控，主客体收益为(0, 0)。

3　容器权限控制博弈奖惩约束机制

3.1　条件假设

在访问过程中，若访问主体为初次提出读取客体容器内文件的请求，本文设定客体容器的初始权限等级处于区间$T_{o\rightarrow s}\in(0.4,0.6)$，当访问客体针对访问主体所计算得出的综合权限评估值达到或超越某一预设标准时（该标准依据客体所含文件的重要性程度而设定，具体表现为最低权限阈值$\theta\in[0,1]$），访问客体将授予该主体以读写特定文件的权限；反之，若综合权限评估值未达此预设标准，则访问请求将被拒绝[27-29]。

进一步而言，若访问主体在上一次访问过程中遵循了受控访问规则，则在本轮权限控制中，应采取奖励机制以资鼓励，并随之授予其访问权限。相反，若访问主体在上一次访问过程中实施了非受控访问行为，则将依据具体情况实施相应惩罚措施，直至永久剥夺其访问客体的权限[30-32]。

获得访问权限的访问主体，在相对于访问客体

的授权行动序列中处于后动地位。在此情境下，以目标导向和收益最大化为原则的访问主体，其行动策略的选择应当符合理性逻辑。然而，为确保访问行为的合规性，需引入触发策略作为约束机制。具体而言，一旦访问主体发生非受控访问行为，将触发约束机制对其施加相应惩罚，直至永久撤销其访问权限。此过程涉及利用访问反馈等后验信息，对访问客体针对该访问主体的权限调整策略 $T_{O\xrightarrow{I}S}\geqslant 0$（其中 I 代表访问次数）进行动态修正，或提高对该访问主体的相关访问权限阈值 θ<1，以强化访问控制的有效性。

3.2 奖惩约束机制

奖惩约束机制是一种反馈控制机制，如果访问主体容器在访问客体宿主机的相关文件时能够按照授权范围进行受控访问，将通过奖励因子 φ 适当提高访问主体的访问权限等级，以提高主体容器的可读取文件范围，使其能完成更多的处理任务，如果访问主体进行授权范围外的非受控访问，则视情况对其加以处罚，降低其访问权限等级，直到其不可访问该客体宿主机内任何文件为止[33-34]。

1) 奖励约束机制。当访问主体容器进行受控访问时，奖励约束机制通过提高其访问权限等级来激励访问主体容器，提高其访问权限值，使其能够访问更高级别的文件[35]。

假设 α 是读写权限，δ 是只读权限，γ 是容器的属性因素，p 是受控访问概率，奖励因子 φ（0≤φ≤1）可以表示为 $\varphi(\alpha,\delta,\gamma,p)$。

在控制其他相关变量恒定不变的条件下，参数 φ 会依据多种影响因素的动态变化而进行适应性调整，其值呈现随参数 α、δ 和 γ 的递增而持续增大的趋势。基于既定假设条件，在面向客运服务领域的云边端协同架构场景中，该参数 φ 能够有效且准确地映射出主体容器访问行为的受控程度以及权限激励机制的实施效果。

在主客体数据交互的动态过程中，设定访问主体的奖励因子为 φ（其中 φ 的取值范围限定为0≤φ≤1），那么在 t_1 时刻，访问主体若选择采取受控访问策略，其所获得的预期收益可表示为

$$R_{ho}^{t_1}=pS_{t,i}+(1-p)S_{tn,i} \tag{1}$$

则 t_i 时刻访问主体容器选择受控访问模式的预期总回报收益为

$$R_{ho}^{t_i}=R_{ho}^{t_{i-1}}(1+\varphi)\frac{pS_{t,i}+(1-p)S_{tn,i}}{1-\varphi} \tag{2}$$

则当前访问主体容器选择不受控访问模式的预期收益为

$$R_{di}=pS_{tn,l}+(1-p)S_{t,l} \tag{3}$$

根据博弈原则可知

$$\begin{cases}R_{di}>R_{ho}^{t_i},S_s=\text{不受控}\\ R_{di}=R_{ho}^{t_i},S_s=\text{不受控}\|\text{受控}\\ R_{di}<R_{ho}^{t_i},S_s=\text{受控}\end{cases} \tag{4}$$

由此可见，当访问主体选择不受控访问模式所获得的预期收益，高于其选择受控访问模式所预期的总回报收益时，访问主体将倾向于采取不受控策略。若2种访问模式下访问主体的预期收益相等，即不受控访问模式的预期收益与受控访问模式的预期总回报收益持平，此时访问主体在策略选择上可能存在不确定性，既可能选择不受控策略，也可能倾向于受控策略。而当访问主体选择不受控访问模式的预期收益，低于其选择受控访问模式所预期的总回报收益时，访问主体将始终倾向于选择受控策略与访问客体进行交互，以此实现其回报收益最大化。

因此，选择合适的奖励因子 φ（0≤φ≤1），满足如式(5)所示约束条件时。

$$\varphi>1-\frac{P(S_{t,i}-S_{tm,i})}{P(S_{t,i}-S_{tn,l})-S_{t,l}} \tag{5}$$

只要访问主体容器追求收益最大化获得更多的计算任务，选择的访问行为策略就永远受控。

2) 惩罚约束机制。惩罚约束机制的核心在于，当访问主体作出不受控访问策略选择时，惩罚约束机制将启动相应惩处措施，具体表现为削减访问主体的收益所得，同时下调其访问权限等级，致使该访问主体因权限不足而无法访问其申请获取的文件资源。

在访问主体实施不受控访问行为之后，惩罚约束机制将依据具体情形，采取以下差异化策略进行应对。

策略 a（温和策略）[36]。提高访问客体的访问权限阈值 θ 值，降低访问主客体容器和宿主机的收益 U，从而降低访问客体对访问主体的相关权限 $T_{O\xrightarrow{I}S}$。

策略 b（严厉策略）[37]。当访问权限值 $T_{O\to S}$<

θ或不受控访问行为发生的次数k大于访问控制机制事先设定的最大容忍最小触发值N_m（本文为3）时，永远被禁止访问客体。

因此，访问客体依据访问主体所实施的不受控访问行为所造成的危害程度，依照式(6)所规定的规则来执行相应的策略抉择。

$$S_o(s)\begin{cases} a, T_{O\to S} \geqslant \theta \| k < N_m \\ b, T_{O\to S} < \theta \| k \geqslant N_m \end{cases} \tag{6}$$

随着惩罚约束机制被纳入控制体系，具备理性思维的文件访问交互节点在决策过程中必然需要权衡当前行为对后续博弈阶段所产生的连锁影响。具体而言，对于那些采取不受控访问策略的访问主体而言，其在第t个访问阶段所面临的预期损失，实质上是该主体在各个访问阶段所累积损失的总和，可表示为

$$U_{s1}(t) = \sum_{k=1}^{\infty} \frac{1}{\beta^{k-1}} u_s(k) \tag{7}$$

其中，$\beta \in (0,1)$为惩罚因子，U、β和k之间取值关系如图3所示，β越小，不受控访问的主体容器累积损失越大，表示惩罚越严厉，它的值由面向客运服务的云边端协同架构中容器本身的各个因素决定。$u_s(k)$为访问主体容器在第k阶段的收益损失。

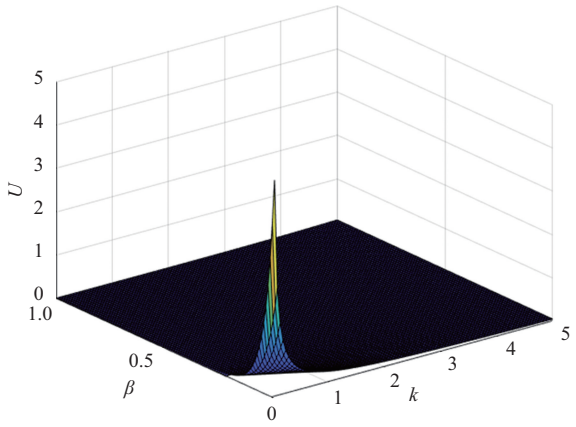


图3　U、β和k之间取值关系

将表1基于权限的访问控制博弈支付矩阵中的相关参数代入$U_{s1}(t)$得

$$U_{s1}(t) = \sum_{k=1}^{\infty} \frac{1}{\beta^{k-1}} \left(pO_{t,l} + (1-p) O_{tm,l} \right) k \tag{8}$$

基于前文分析推导可知，当数据访问主体容器由受控访问状态转变为不受控访问状态时，该节点能够借助博弈分析方法精确计算出自身在此转变过程中可能遭受的最大收益损失，进而据此推算出其在实施不受控访问行为后，第t+1个阶段的收益值$U_s(t+1)$，其计算式为$U_s(t+1)=U_s(t)-U_{s1}(t)$。同时，可基于上述分析评估得出综合权限评估值$T_{O\to S}$，判断其是否小于阈值$\theta$。

此外，还需明确惩罚阶段的时间周期参数n。通过系统灵活调整参数n的大小，能够显著增强系统机制对不受控访问行为的惩处力度。这一机制不仅可作为系统安全保障的应急措施，有效提升系统机制的整体安全性，还能最大程度地降低客体因不受控行为而遭受的最小损失，进而有效遏制访问主体从受控访问行为向不受控访问行为的转变趋势，对具有恶意不受控访问行为的访问主体容器形成了强有力的威慑效应。

3.3　奖惩约束机制算法

根据上文奖惩约束机制设计思想，本节给出奖惩约束机制的算法流程[38]，如图4所示。

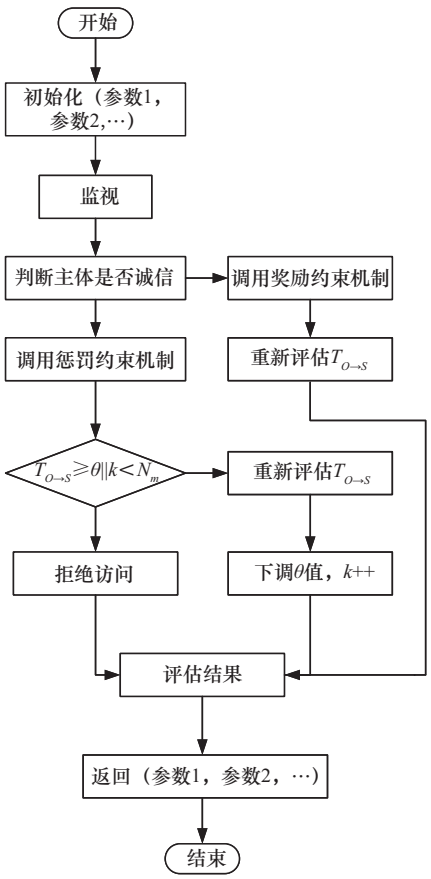


图4　奖惩约束机制算法流程

1) 初始化阶段，访问的主客体容器和宿主机处于访问等待状态，同时云边端协同平台的权限调

整系统处于监视状态，从博弈模型中获取初始化参数（$N, S, p, \cdots, T$），评估判断容器的可信程度和受控情况。

2) 当访问的主体容器受控访问客体宿主机内文件时，触发奖励约束机制；判断相关收益所满足的条件，由系统设置合适的奖励因子φ，奖励主体自觉选择受控访问转向4)。

3) 当访问的主体容器不受控访问客体宿主机时，触发惩罚约束机制；判断不受控行为的程度，并给出对应的惩罚力度；当$T_{O\to S}<\theta \| k\geqslant N_m$时，惩罚力度最大直接拒绝访问。

4) 重新对主客体容器和宿主机进行权限设置，反馈相关参数，流程结束。

4　仿真分析

4.1　仿真实验参数

为了验证本文机制的有效性，假设访问的容器和宿主机之间博弈的支付矩阵如表3所示。

表3　　容器和宿主机之间博弈的支付矩阵

参与方		宿主机E_j		
		访问行为	授权	拒绝
容器E_i	可信	受控	（5, 5）	（0, –5）
	可信	不受控	（10, 0）	（0, 5）

其他仿真参数设置如下：假设访问宿主机的容器共12个，其中1、2、3、5和9是有逃逸风险的恶意容器；假设N_m=3，θ=0.5，$\alpha>0$，$\beta>0$，p=1。

文件访问过程中主客体容器和宿主机之间的访问权限阈值动态变化可用式(9)表示。

$$f(\theta)=\theta(1-\theta)\left[\theta\left(E_{ho}+\alpha T-E_{di}\right)\right]+(1-\theta)\left[\theta\left(E_{ho}+\alpha T-E_{di}-U_{sl}(t)\right)\right] \tag{9}$$

其中，E_{ho}为受控访问的收益，可表示为

$$E_{ho}=S_{t,i}(1+\varphi+\varphi^2+\cdots+\varphi^t+\varphi^{t+1}+\cdots)=S_{t,i}\frac{1-\varphi^{t-1}}{1-\varphi}+S_{t,i}\varphi^{t-1}+S_{t,i}\frac{\varphi^t}{1-\varphi} \tag{10}$$

其中，E_{di}为非受控访问的收益，可表示为

$$E_{di}=S_{t,i}(1+\varphi+\varphi^2+\cdots+\varphi^{t-2})+S_{tn,i}\varphi^t=S_{t,i}\frac{1-\varphi^{t-1}}{1-\varphi}+S_{tn,i}\varphi^{t-1} \tag{11}$$

因此，只有$E_{ho}>E_{di}$时才会激励容器选择受控方式访问文件。奖励因子通过增加访问文件的容器权限，激励访问主体容器的受控访问，相反惩罚因子是通过降低访问文件的容器权限来制裁容器。惩罚因子计算方式类似，故不再赘述。

4.2　奖惩效果分析

根据权限阈值动态变化计算方法，图5和图6给出了文件访问的主客体容器和宿主机在相同初始权限下的演化。由图5可知，在初始值（0.5）不变的情况下，α=0.3时对应的文件访问的主体容器和客体宿主机权限演化曲线收敛到稳定状态且取得最高权限的速度明显快于α=0.2时的收敛速度，α=0.2时对应的文件访问的主客体容器和宿主机权限演化曲线收敛到稳定状态且取得最高权限的速度明显快于α=0.1时的收敛速度。

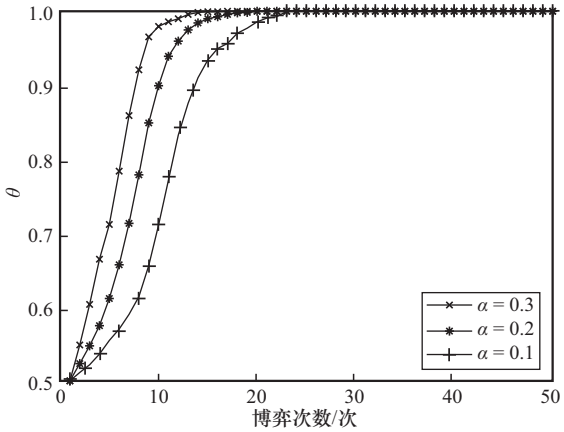


图5　奖励约束机制下权限的演化

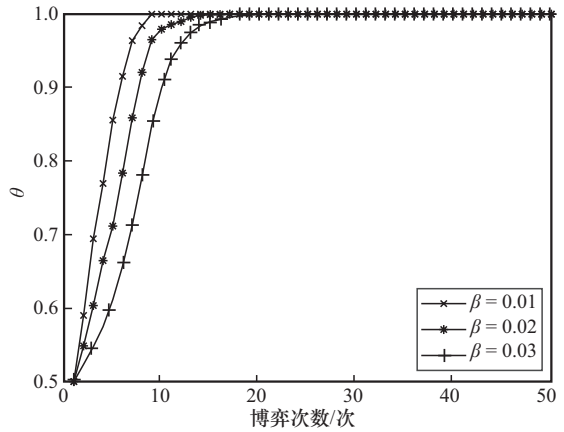


图6　惩罚约束机制下权限的演化

从图6可以看出，在初始值（0.5）不变的情况下，β=0.01时对应的文件访问的主客体容器和宿主机权限演化曲线收敛到稳定状态且取得最高权限的速度明显快于β=0.02时的收敛速度，β=0.02时对应

的文件访问的主客体容器和宿主机权限演化曲线收敛到稳定状态且取得最高权限的速度明显快于β=0.03时的收敛速度。

由此可见读写权限α的取值越大，博弈过程的收敛速度越快，系统对访问权限的纠正速度越快。惩罚因子β的取值越小，博弈过程的收敛速度越快，系统对访问权限的纠正速度越快。

4.3　奖惩约束机制性能分析

为更清晰地阐释奖惩约束机制的实际效果，本文借助实验数据进行了对比分析。实验设定了2种情境：一种情境下未实施奖惩约束机制，另一种情境下则引入了奖惩约束机制。实验中，将申请访问文件的主体划分为两类：主体4、6、7、8、10、11和12被设定为受控容器，主体1、2、3、5和9则被设定为不受控容器。每个任务均需执行5次文件访问操作。实验结果显示，在第1个任务周期内，不同容器访问文件所获得的预期收益存在差异，具体数据如图7所示。

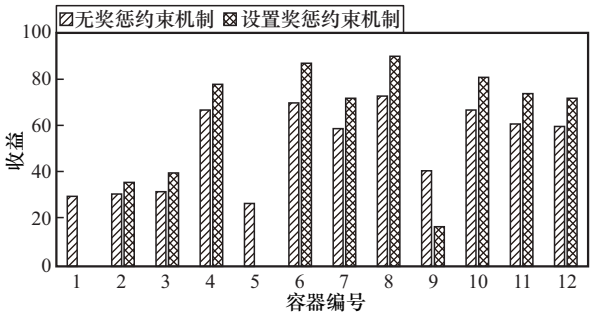


图7　访问主体预期收益

从图7中可以明确观察到，对于受控容器（即主体4、6、7、8、10、11和12）而言，在设置奖惩约束机制的情况下，其预期收益始终超越无奖惩约束机制时的预期收益水平。而对于不受控容器（主体1、2、3、5和9），奖惩约束机制对其产生了多样化的影响，节点1和节点5因实施了不受控的访问操作，触发了惩罚约束机制，导致其收益受到削减，并且这2个容器被直接拒绝访问；容器9虽也出现了不受控访问行为，但惩罚约束机制及时介入，有效阻止了其后续的不当访问尝试；容器2和容器3未发生不受控的访问行为，因此奖励约束机制得以发挥积极作用，成功实现了预期的奖励目标。

图8呈现了容器（编号为1~12）访问宿主机文件的访问成功率随访问周期变化的规律。从图8中可观察到，在本文机制、文献[39]、文献[40]及文献[41]所描述的惩罚奖励机制下，容器访问宿主机文件的访问成功率均高于无奖惩约束机制时的成功率，传统ABAC机制和中国墙混合访问控制机制下访问成功率保持稳定，不具备动态适应和调整能力。具体而言，在本文机制的作用下，随着访问周期的推进，容器访问宿主机文件的访问成功率显著提升并逐渐趋于稳定；在文献[39]、文献[40]及文献[41]的惩罚奖励机制下，容器访问宿主机文件的访问成功率虽在访问周期存在较大波动，但整体上保持平稳，本文机制访问成功率稳步提升，且波动较小。相比之下，在无奖惩约束机制的情况下，容器访问宿主机文件的访问成功率随访问周期的延长而明显下降，直至达到稳定状态。因此，在基于云边端的客运服务平台容器访问控制中，设计针对文件访问去向的容器与宿主机权限奖惩约束机制是行之有效的。

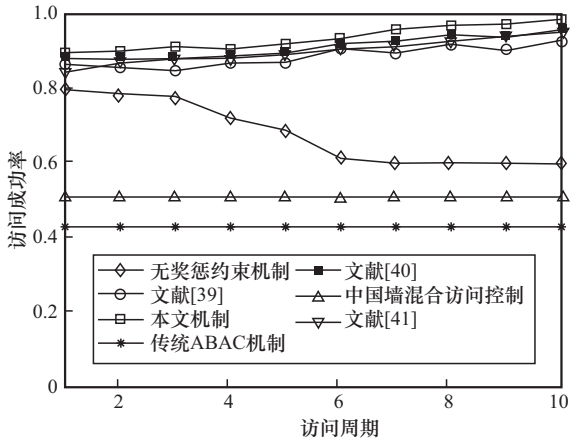


图8　访问成功率

图9展示了容器访问宿主机文件的访问成功率与不受控节点比例之间的关系。从图9中可知，随着不受控节点的增多，容器访问宿主机文件的访问成功率逐渐降低。在本文机制有效运行的情况下，当不受控节点占比达到40%时，容器访问宿主机文件的访问成功率将降至0.5以下，此时访问成功率显著下降，从而有效保障了文件访问（此处结合语境实际想表达的是保障了访问宿主机相关操作的安全性，若严格对应替换逻辑可表述为保障了涉及宿主机文件访问场景下的安全性）的安全性。而在无奖惩约束机制的情况下，随着不受控节点比例的增加，容器访问宿主机文件的访问成功率下降速度明显快于本文机制下的情况。

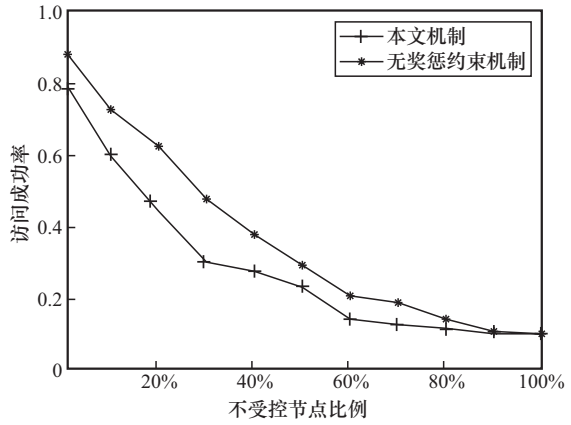


图9　不受控节点的访问成功率

图10展示了在不同容器数量情况下的内存访问开销变化规律，从图中可以看出，初始统计访问客体宿主机的主体容器数量是100个，依次变化到访问客体宿主机的主体容器数量为1 000个，其变化规律是随着访问客体宿主机的主体容器数量的增加，内存访问开销呈线性增大变化；同样情况下无奖惩约束机制下不同访问客体宿主机的主体容器数量的内存访问开销变化规律，二者相比较表明本文机制下在主体任务周期内访问客体宿主机文件时产生的内存访问开销是符合实际的，但由于机制的存在会产生额外的内存访问开销，且访问频率可控，因此，该机制具有很好的可行性。

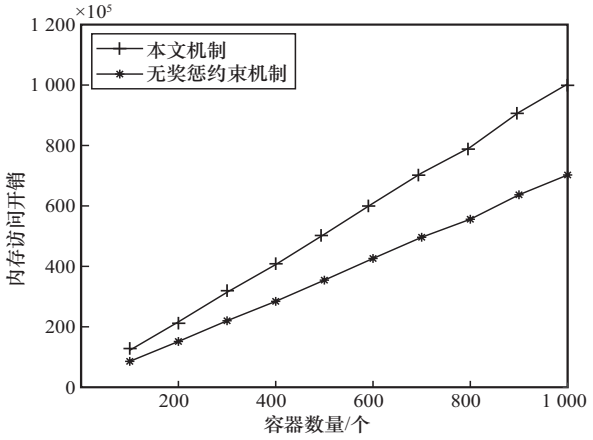


图10　内存访问开销

在金牌6 330×2/128 GB/960 GB×2+8 TB×3宿主机中配置相同容器，在不同安全策略下连续执行100次任务的平均执行耗时如表4所示。本文机制在客票验证、人像识别及购票查询任务下增加任务执行耗时4.67%，相较混合访问控制增加任务执行耗时0.67%。总体而言，本文机制对任务执行耗时影响较小，但仍有进一步优化空间。

表4　任务执行耗时

策略	客票验证任务/ms	人像识别任务/ms	购票查询任务/ms
无安全防护	577	6 373	217
本文机制	693	6 487	322
混合访问控制	688	6 444	320

5　结束语

本文首先建立基于云边端协同架构的客运服务系统业务场景下的权限控制博弈模型。在传统ABAC基础上动态控制客体容器的访问权限，以最大限度地降低容器逃逸对宿主机及其他共享资源容器的影响，然后将博弈引入容器权限动态调整中，设计基于奖惩机制的访问权限控制博弈约束机制，以权限激励驱动，奖励受控容器，惩罚有逃逸倾向的容器，实现基于权限控制实现处理能力与安全隔离的总体均衡，最后通过仿真实验分析得出以下结论。

1) 本文机制收敛速度受奖励因子和惩罚因子的权重影响，奖励因子和惩罚因子权重越大收敛速度越快。

2) 相较于传统权限控制方式，基于奖惩机制的访问权限控制博弈约束机制可以更灵活地调整访问权限，使不受控访问变少，证明该方法具有有效性。

3) 本文机制虽然会增加内存读取的负担，但是整体处于可控状态，不会使内存读取呈数量级增加。

4) 本文机制以牺牲任务执行效率为代价换取容器安全隔离强度，对任务执行耗时影响较小控制在5%以下，但仍有进一步优化空间。

由于作者能力和篇幅有限，本文未对容器安全隔离机制下的任务执行各阶段效率进行研究，未分析本文机制对任务执行各阶段的影响，因此后续将对此开展研究，以提升本文机制的应用价值。

参考文献：

[1] CAO Y, WEN J K, HOBINY A, et al. Parameter-varying artificial potential field control of virtual coupling system with nonlinear dynamics[J].

Fractals, 2022, 30(2): 2240099.

[2] CAO Y, LI P, ZHANG Y Z. Parallel processing algorithm for railway signal fault diagnosis data based on cloud computing[J]. Future Generation Computer Systems, 2018, 88: 279-283.

[3] 罗潇, 刘悦. 轨道交通车载端到端语音合成[J]. 机车电传动, 2023(6): 122-128.
LUO X, LIU Y. An end-to-end text-to-speech system for vehicle-mounted devices[J]. Electric Drive for Locomotives, 2023(6): 122-128.

[4] 龙腾, 王彧弋, 林军, 等. 轨道交通车载智能化应用技术发展展望[J]. 机车电传动, 2024(1): 11-21.
LONG T, WANG Y Y, LIN J, et al. Development review and prospects of intelligent technology in rail transit vehicles[J]. Electric Drive for Locomotives, 2024(1): 11-21.

[5] 贺佳. 基于三维点云与图像融合的轨道交通场景行人检测方法[J]. 机车电传动, 2024(3): 146-155.
HE J. Pedestrian detection method in rail transit scenes based on fusion of 3D point clouds and images[J]. Electric Drive for Locomotives, 2024(3): 146-155.

[6] 李佳曦. 基于容器技术的云化平台安全风险与应对分析[J]. 信息通信技术, 2020, 14(6): 26-31, 38.
LI J X. Security risks and countermeasures analysis of cloud platform based on container technology[J]. Information and Communications Technologies, 2020, 14(6): 26-31, 38.

[7] JIANG W H, LI Z. Vulnerability analysis and security research of docker container[C]//Proceedings of the 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE). Piscataway: IEEE Press, 2020: 354-357.

[8] ZEROUALI A, MENS T, ROOVER C D. On the usage of JavaScript, Python and Ruby packages in Docker Hub images[J]. Science of Computer Programming, 2021, 207: 102653.

[9] LIU P Y, JI S L, FU L R, et al. Understanding the security risks of docker hub[C]//Computer Security-ESORICS 2020. Berlin: Springer, 2020: 257-276.

[10] 张云涛, 方滨兴, 杜春来, 等. 基于异构观测链的容器逃逸检测方法[J]. 通信学报, 2023, 44(1): 49-63.
ZHANG Y T, FANG B X, DU C L, et al. Container escape detection method based on heterogeneous observation chain[J]. Journal on Communications, 2023, 44(1): 49-63.

[11] 胥柯, 张新有, 栗晓晗. Docker容器逃逸防护技术研究[J]. 信息安全研究, 2022, 8(8): 768-776.
XU K, ZHANG X Y, LI X H. Research on the escape protection of docker container[J]. Journal of Information Security Research, 2022, 8(8): 768-776.

[12] 王杰, 巨汉基, 杜跃, 等. 基于Docker容器行为分析的安全隔离系统[J]. 浙江电力, 2022, 41(5): 96-102.
WANG J, JU H J, DU Y, et al. A security isolation system based on docker container behavior analysis[J]. Zhejiang Electric Power, 2022, 41(5): 96-102.

[13] 陈红松, 陈京九. 基于统计的物联网分布式拒绝服务攻击检测[J]. 吉林大学学报(工学版), 2020, 50(5): 1894-1904.
CHEN H S, CHEN J J. Statistical based distributed denial of service attack detection research in Internet of things[J]. Journal of Jilin University (Engineering and Technology Edition), 2020, 50(5): 1894-1904.

[14] 季一木, 杨卫东, 李奎, 等. 基于主机系统调用频率的容器入侵检测方法[J]. 网络与信息安全学报, 2021, 7(4): 18-29.
JI Y M, YANG W D, LI K, et al. Container intrusion detection method based on host system call frequency[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 18-29.

[15] BUI T. Analysis of docker security[J]. arXiv Preprint, arXiv: 1501.02967, 2015.

[16] RESHETOVA E, KARHUNEN J, NYMAN T, et al. Security of OS-level virtualization technologies[C]//Secure IT Systems. Berlin: Springer, 2014: 77-93.

[17] BACIS E, MUTTI S, CAPELLI S, et al. DockerPolicyModules: mandatory access control for docker containers[C]//Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS). Piscataway: IEEE Press, 2015: 749-750.

[18] MILLER A, CHEN L. Securing your containers: an exercise in secure high performance virtual containers[C]//Proceedings of the International Conference on Security and Management (SAM), 2012, 1.

[19] JIAN Z Q, CHEN L. A defense method against docker escape attack[C]//Proceedings of the 2017 International Conference on Cryptography, Security and Privacy. New York: ACM Press, 2017: 142-146.

[20] CHELLADHURAI J, CHELLIAH P R, KUMAR S A. Securing docker containers from denial of service (DoS) attacks[C]//Proceedings of the 2016 IEEE International Conference on Services Computing (SCC). Piscataway: IEEE Press, 2016: 856-859.

[21] ABIDRABBU S, ABUSHATTAL A, ARSLAN H. Stackelberg game for secure CR-NOMA networks against internal eavesdropper[J]. IEEE Transactions on Cognitive Communications and Networking, 2023, 9(2): 452-462.

[22] LU T, CHEN J. Research of penetration testing technology in docker environment[C]//Proceedings of the 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017). Atlantis Press, 2017: 1354-1359.

[23] MOUAT A. Docker security: using containers safely in production[M]. Sebastopol: O'Reilly Media, 2015.

[24] DREW F, JEAN T. Game theory[M]. Cambridge, Mass. MIT Press, 1991: 275-277.

[25] 赵斌, 何泾沙, 张伊璇, 等. 基于灰色关联分析的推荐信任评估方法[J]. 北京大学学报(自然科学版), 2017, 53(2): 314-320.
ZHAO B, HE J S, ZHANG Y X, et al. The method of recommended trust evaluation based on grey correlation analysis[J]. Acta Scientiarum Naturalium Universitatis Pekinensis, 2017, 53(2): 314-320.

[26] GHARAM M, ABDALLAH W, BOUDRIGA N. The design of a game-theoretic based multiple access scheme for 5G millimeter wave communication networks[C]//Proceedings of the 15th International Conference on Advances in Mobile Computing & Multimedia. New York: ACM Press, 2017: 166-174.

[27] 刘琴, 刘旭辉, 胡柏霜, 等. 个人健康记录云管理系统中支持用户撤销的细粒度访问控制[J]. 电子与信息学报, 2017, 39(5): 1206-1212.
LIU Q, LIU X H, HU B S, et al. Fine-grained access control with user revocation in cloud-based personal health record system[J]. Journal of Electronics & Information Technology, 2017, 39(5): 1206-1212.

[28] 郭树行, 张禹. 基于动态情景网关的系统协同访问控制模型[J]. 通信学报, 2013, 34(S1): 142-147.
GUO S H, ZHANG Y. Dynamic situation gateway based system cooperation access gatel model[J]. Journal on Communications, 2013, 34 (S1): 142-147.

[29] HELIL N, HALIK A, RAHMAN K. Non-zero-sum cooperative access control game model with user trust and permission risk[J]. Applied Mathematics and Computation, 2017, 307: 299-310.

[30] CHEN L J, LOW S H, DOYLE J C. Random access game and medium access control design[J]. IEEE/ACM Transactions on Networking, 2010, 18(4): 1303-1316.

[31] KISHOR A, NIYOGI R. A game-theoretic approach to solve the free-rider problem[C]//Proceedings of the 2017 Tenth International Conference on Contemporary Computing (IC3). Piscataway: IEEE Press, 2017: 1-6.

[32] ZHAO B, XIAO C B, ZHANG Y, et al. Assessment of recommendation trust for access control in open networks[J]. Cluster Computing, 2019, 22(1): 565-571.

[33] 郭子溢, 刘立, 叶牡丹, 等. 层次化社交网络中直销激励机制的研究与设计[J]. 计算机工程与设计, 2017, 38(8): 2111-2115.
GUO Z Y, LIU L, YE M D, et al. Research and design of direct marketing incentive system in hierarchical social network[J]. Computer Engineering and Design, 2017, 38(8): 2111-2115.

[34] ALLADI T, CHAMOLA V, SAHU N, et al. A comprehensive survey on the applications of blockchain for securing vehicular networks[J]. IEEE Communications Surveys and Tutorials, 2022, 24(2): 1212-1239.

[35] WANG R, WANG D T. Research on key technologies of cooperative spectrum sensing based on game theory[C]//Proceedings of the 2025 5th International Conference on Consumer Electronics and Computer Engineering (ICCECE). Piscataway: IEEE Press, 2025: 195-198.

[36] LI F S, LIN R Q, CHEN W C, et al. Thwarting SSDF attacks from high-speed movement VUs in the CIoV network: based on blockchain and stochastic evolutionary game[J]. IEEE Internet of Things Journal, 2025, 12(2): 2233-2250.

[37] 王博, 黄传河, 杨文忠, 等. Ad Hoc网络中基于惩罚机制的激励合作转发模型[J]. 计算机研究与发展, 2011, 48(3): 398-406.
WANG B, HUANG C H, YANG W Z, et al. An incentive-cooperative forwarding model based on punishment mechanism in wireless Ad Hoc networks[J]. Journal of Computer Research and Development, 2011, 48(3): 398-406.

[38] 王杨, 王汝传, 徐小龙, 等. 资源共享P2P网络的进化博弈激励模型[J]. 计算机工程, 2011, 37(11): 19-21.
WANG Y, WANG R C, XU X L, et al. Evolutionary game incentive model for resource sharing P2P network[J]. Computer Engineering, 2011, 37(11): 19-21.

[39] HOU H F, LIN R Q, WANG J, et al. Blockchain and game theory-based strategies for anti-jamming and eavesdropping in EH-CR networks[J]. IEEE Access, 2024, 12: 146996-147011.

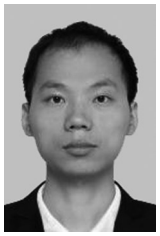
[40] 吕兴昱. 基于博弈论的联邦学习内在激励机制研究[D]. 广州大学, 2023.
LYU X Y. Research on intrinsic incentive mechanism of federated learning based on game theory[D]. Guangzhou University, 2023.

[41] SUN Y X, JIANG W J, YANG Y, et al. Multi-domain authorization and decision-making method of access control in the edge environment[J]. Computer Networks, 2023, 228: 109721.

[作者简介]

温佳坤（1996– ），男，河北唐山人，北京交通大学博士生，北京全路通信信号研究设计院集团有限公司工程师，主要研究方向为云平台安全保障、高速铁路列车运行控制等。

曹源（1982– ），男，河南开封人，博士，北京交通大学教授、博士生导师，主要研究方向为列车运行控制系统健康管理。



孙永奎（1993– ），男，河南永城人，博士，北京交通大学副教授，主要研究方向为列车运行控制系统故障诊断、云平台安全保障。

王峰（1986– ），男，河北石家庄人，博士，北京交通大学副教授，主要研究方向为高维数据的统计建模和预测、云平台安全保障。

邱兆阳（1975– ），男，山东青岛人，北京全路通信信号研究设计院集团有限公司工程师，主要研究方向为安全云平台、高速铁路信号系统安全保障。