面向边缘计算的容器编排安全部署方案研究

李晓荣
内蒙古电子信息职业技术学院　内蒙古　呼和浩特　010020

摘　要：随着边缘计算的广泛应用，容器编排在其中的重要性日益凸显，但安全问题也随之而来。本文首先分析了边缘计算环境下容器编排的安全需求，涵盖容器镜像、编排平台、网络通信和数据安全等方面。接着从这四个方面提出具体安全部署方案，随后阐述方案的评估，包括有效性、性能评估，探讨安全性与性能平衡及方案扩展性和适应性，给出扩展和改进建议，为边缘计算环境下容器编排安全部署提供全面参考。

关键词：边缘计算；容器编排；安全部署；方案研究

引言：在边缘计算广泛应用的当下，容器编排成为关键支撑，但安全问题日益凸显。边缘计算环境资源受限、分布广泛等特性，以及容器编排在物联网、智能交通等领域的应用，使其面临容器镜像篡改、编排平台漏洞、网络通信攻击、数据泄露等诸多安全威胁。本文聚焦面向边缘计算的容器编排安全部署方案，深入分析安全需求，提出具体部署策略，并对方案有效性、系统性能、安全性与性能平衡、扩展性和适应性进行评估，为相关安全实践提供参考。

1 边缘计算环境下容器编排的安全需求分析

边缘计算环境下容器编排存在特定安全需求，这与其环境特点、应用场景及面临的安全威胁紧密相关。边缘计算环境有资源受限、网络不稳定、设备异构、分布广泛等特性，易遭受恶意攻击、数据泄露等安全威胁。容器编排在边缘计算中应用于物联网、智能交通、工业互联网等领域，在物联网中能统一管理调度大量边缘设备，在智能交通中可支持实时交通数据处理与智能决策[1]。其面临多种安全威胁，容器镜像方面存在被篡改、植入恶意代码风险，会使容器应用运行时遭到攻击；编排平台可能有漏洞，被攻击者利用进行非法操作，如控制容器、窃取数据；网络通信易受中间人攻击、数据截取威胁，导致数据泄露篡改；边缘设备产生的数据含大量敏感信息，如用户隐私、商业机密，需保障其保密性、完整性和可用性。基于这些，边缘计算环境下容器编排有明确安全需求，容器镜像安全要确保完整性和真实性，防止被篡改和植入恶意代码；编排平台安全需保障自身安全性，防止攻击者利用漏洞非法操作；网络通信安全要保证边缘计算环境网络通信安全，防止数据传输时泄露篡改；数据安全要保护边缘设备产生的数据，确保其保密性、完整性和可用性，以维护边缘计算环境下容器编排系统的稳定安全运行。

2 面向边缘计算的容器编排安全部署方案

2.1 容器镜像安全

（1）镜像签名与验证，是保障镜像完整性和真实性的关键手段，通过数字签名技术为容器镜像赋予唯一标识，在部署前严格验证镜像签名，能有效防止镜像在传输或存储过程中被篡改，确保用户获取到的是未经修改、来源可信的原始镜像，避免因使用被篡改镜像而引发的安全风险，如恶意代码植入、数据泄露等。（2）镜像扫描与漏洞检测，及时发现并处理镜像安全隐患的重要措施，借助专业的镜像扫描工具，对容器镜像进行全面细致的扫描，精准检测其中存在的各类漏洞和潜在恶意代码[2]。一旦发现问题，及时采取修复措施，如更新软件版本、移除恶意代码等，保证镜像的安全性，防止攻击者利用镜像漏洞入侵系统，保障边缘计算环境的安全稳定。（3）镜像存储安全，将容器镜像存储于安全的存储系统中，运用访问控制技术，严格限制对镜像的访问权限，只有授权用户和系统才能进行读取、写入等操作；同时采用加密技术对镜像数据进行加密处理，即使存储设备被盗取或数据在传输过程中被截获，攻击者也无法获取镜像的真实内容，有效保障镜像在存储阶段的安全性，为容器编排提供安全可靠的镜像支持。

2.2 编排平台安全

平台认证与授权是安全防护首要关卡，要对所有访问编排平台的用户和设备执行严格认证流程，用身份验证、多因素认证确认合法性，依据预设权限策略授予相应权限，确保只有合法主体进入，防止非法接入导致数据泄露、恶意操作等风险。平台漏洞管理是持续维护安全重要举措，因软件系统有漏洞隐患，编排平台也是如此，要定期用专业工具全面检测，精准识别潜在漏洞，依据严重程度和影响范围及时制定修复方案，通过装官方补丁、更新版本等消除漏洞，避免攻击者利用提权、

植入恶意代码等，保障运行稳定安全。安全审计与监控是及时发现和处理安全问题重要手段，要建立完善审计机制，详细记录平台上用户登录、资源分配、任务调度等关键操作信息，同时用实时监控技术持续监测运行状态和操作行为，设定安全基线和异常行为规则，发现偏离正常模式或违反策略的异常行为立即触发预警，安全管理人员迅速响应，深入调查分析，采取阻断操作、隔离设备等措施及时处理，防止安全事件扩大，全方位保障编排平台安全。

2.3 网络通信安全

（1）加密通信，保障数据传输安全的基础手段，采用SSL/TLS等成熟加密协议，对边缘计算环境内的网络通信进行加密处理。在数据传输过程中，这些协议会将数据转化为密文，即使数据被恶意截取，攻击者也无法获取其中的真实内容，有效防止数据泄露与篡改，确保数据从发送端到接收端的安全传输。（2）网络隔离，通过虚拟专用网络（VPN）等技术实现不同网络间的有效隔离。在边缘计算环境中，可能存在多个不同安全级别的网络，如业务网络、管理网络等。利用VPN技术可构建安全的逻辑通道，将不同网络分隔开来，限制网络间的非法访问与数据流动，防止攻击者通过网络渗透手段，从一个网络侵入另一个网络，降低安全风险，保障各网络的独立性与安全性。（3）入侵检测与防御，应对网络攻击的关键防线，部署入侵检测系统（IDS）和入侵防御系统（IPS），对网络流量进行实时、全面的监测与分析。IDS能够及时发现网络中的异常行为与潜在入侵迹象，发出预警信号；IPS则可在检测到入侵行为时，自动采取阻断措施，阻止攻击的进一步发展，有效保护边缘计算环境的网络通信安全，确保容器编排系统的稳定运行。

2.4 数据安全

数据加密是保障数据安全的基础防线，针对边缘设备产生的各类敏感数据，如用户身份信息、业务交易记录等，采用高强度加密算法进行加密处理。在数据存储阶段，加密后的数据以密文形式存在，即便存储设备被盗取或存储环境被非法访问，攻击者也无法获取数据的真实内容；在数据传输过程中，加密能防止数据在公网等不安全网络中被截获和篡改，确保数据的保密性和完整性[3]。数据备份与恢复是应对数据丢失或损坏风险的重要手段，定期对边缘设备的数据进行全面备份，将备份数据存储在安全可靠的位置，如异地数据中心或云端。同时建立完善的数据恢复机制，当遭遇自然灾害、设备故障或人为误操作等导致数据丢失或损坏时，能够迅速从备份中恢复数据，最大程度减少数据丢失对业务的影响，保障业务的连续性。数据访问控制是防止数据泄露和滥用的关键环节，通过严格的身份认证和授权机制，对数据的访问进行精细管控。只有经过授权的用户和设备，依据其角色和权限，才能访问相应的数据，且访问过程会被详细记录。这种严格的访问控制能有效阻止非法访问和越权操作，确保数据仅在合法范围内使用，维护数据的安全性和合规性。

3 面向边缘计算的容器编排安全部署方案的评估

3.1 有效性评估

其一要进行安全指标定义，依据容器编排安全核心需求明确可量化、具有代表性指标，如镜像完整性验证成功率反映镜像传输与存储未被篡改程度，是保障容器应用安全启动基础；平台漏洞修复率体现对编排平台漏洞及时处理能力，关乎平台稳定安全；网络通信加密率衡量网络数据传输加密覆盖情况，确保数据传输不被泄露篡改，这些指标为评估安全部署方案提供清晰客观标准。其二是开展实验环境搭建，结合边缘计算实际应用场景构建贴近真实环境的实验平台，在该平台上部署容器编排系统及待评估安全部署方案，保证实验环境能真实反映安全方案实际运行状态与效果，为后续测试分析提供可靠基础。其三进行实验结果分析，在搭建好的实验环境中运用专业测试工具与方法，全面测试安全部署方案各项安全指标，详细记录测试数据，深入分析数据，对比各项指标与预期目标差距，判断安全部署方案是否有效降低安全风险、提升整体安全性，若指标达预期说明方案有效，若存在差距则分析原因并优化改进方案，保障边缘计算环境下容器编排安全部署方案切实发挥作用，确保系统安全稳定运行。

3.2 系统性能评估

（1）进行性能指标定义，明确一系列能精准反映系统性能状况的指标。容器启动时间关乎容器应用能否快速投入运行，启动时间过长会影响业务响应速度；网络延迟体现数据在网络中传输的时效性，对于实时性要求高的业务，如智能交通中的实时数据交互，网络延迟过大可能导致决策失误；系统资源占用率反映安全部署方案对系统资源的消耗情况，若占用过高会挤压其他业务运行所需资源，影响系统整体性能。这些指标为评估安全方案对系统性能的影响提供了量化依据。（2）性能测试方法，选用专业的性能测试工具，在部署安全方案前后分别对系统性能展开测试[4]。通过模拟实际业务场景和数据流量，获取系统在不同状态下的性能数据，如容器启动时间、网络延迟时长、系统资源占用比例等。对部署安全方案前后的测试结果进行详细对比分析，找出性

能变化的关键因素，明确安全方案对系统性能的具体影响程度。（3）性能测试结果提出性能优化建议，若发现加密算法导致网络延迟增加，可考虑优化加密算法，在保证安全性的前提下降低计算复杂度；若安全策略过于严格造成系统资源占用过高，可适当调整安全策略，平衡安全与性能需求。通过这些优化措施，在确保安全部署方案有效性的基础上，提高系统性能，使边缘计算环境下的容器编排系统既能保障安全，又能高效稳定运行。

3.3 安全性与性能的平衡

安全性是保障系统稳定运行、数据安全可靠的核心要素。若过度追求安全性，采用复杂严格的安全技术和策略，如高强度多层加密算法、繁琐访问控制流程等，虽能抵御安全威胁，但会显著增加系统计算开销与资源占用，导致容器启动时间延长、网络通信延迟增加、系统响应速度变慢，影响边缘计算系统性能与业务处理时效性，降低用户体验和业务效率。反之，若为提高系统性能降低安全要求，简化安全防护措施，如减少加密环节、放宽访问权限等，虽能提升系统运行速度与资源利用率，但会使系统暴露于更多安全风险之下，攻击者可能窃取数据、篡改信息或发起恶意攻击，造成数据泄露、系统瘫痪等严重后果，给企业带来巨大经济损失与声誉损害。因此，要实现安全性与性能最佳平衡，需合理选择安全技术和策略，根据系统实际安全需求与性能承受能力，挑选适宜加密算法、访问控制机制等。同时优化系统架构，通过合理资源分配、负载均衡等手段提高系统整体性能，在保障系统具备足够安全防护能力前提下，尽可能降低安全措施对系统性能影响，使边缘计算环境下容器编排系统既能安全稳定运行，又能高效处理业务。

3.4 方案的扩展性和适应性

扩展性主要考量方案随边缘计算规模增长而灵活调整的能力，当边缘节点数量增加、业务数据量扩大时，安全部署方案应能无缝扩展，确保新增节点和数据同样得到有效安全防护，不会因规模扩大而出现安全漏洞或性能瓶颈。适应性则聚焦于方案对不同应用场景的契合度，边缘计算广泛应用于工业互联网、智能交通、智能家居等多个领域，各领域在数据类型、网络环境、安全需求等方面存在差异，安全部署方案须具备足够的灵活性，可根据不同场景特点进行定制化配置，提供针对性的安全保障[5]。为满足未来边缘计算发展需求，需提出扩展和改进建议。在扩展方面，可采用模块化设计理念，将安全功能拆分为独立模块，便于根据规模变化灵活增减模块，如增加数据加密模块以应对数据量增长带来的加密需求。在改进方面，持续跟踪新兴安全技术和标准，将其融入方案中，提升方案对新型安全威胁的防范能力；加强与边缘计算平台和其他相关系统的集成，实现安全信息的共享和协同防护，提高整体安全水平；同时，建立完善的反馈机制，根据实际应用中的问题和需求，及时调整和优化方案，确保安全部署方案始终具备良好的扩展性和适应性，为边缘计算环境的稳定运行和业务发展提供坚实保障。

结束语

综上所述，边缘计算环境下容器编排安全部署方案研究意义重大。通过对安全需求分析，从容器镜像、编排平台、网络通信和数据安全四个方面提出具体方案，并进行全面评估，涵盖有效性、性能、安全性与性能平衡以及扩展性和适应性。该研究为保障边缘计算中容器编排系统安全稳定运行提供了理论支撑与实践指导，有助于推动边缘计算在各领域更安全、高效地应用，促进相关技术不断发展完善。

参考文献：

[1]朱俊涛.边缘计算与新型网络安全体系的融合研究[J].中国信息界,2025,(01):17-19.

[2]龚岩.边缘计算在物联网中的应用研究[J].信息记录材料,2025,26(12):158-160.

[3]李浩.基于物联网的计算机网络工程优化技术分析[J].信息记录材料,2025,26(12):177-179.

[4]杨维荣.基于智能边缘计算的网络安全防护与威胁检测分析[J].电子技术,2024,53(10):256-257.

[5]王贵龙.融合边缘MEC的网络安全部署策略[J].中国电信业,2024,(11):71-74.