边缘计算环境下的网络安全策略与智能决策机制

侯晋成

江苏城乡建设职业学院　213147

摘　要：针对边缘计算中的数据安全挑战，提出了访问控制、数据加密和身份认证等网络安全策略。同时，引入了基于机器学习的智能决策机制，以实现对当前事件的快速响应。通过严格的访问控制策略，确保只有授权用户能访问敏感数据；采用基于多授权方的轻量级数据加密方案，保护数据在传输和存储过程中的机密性；身份认证策略则确保设备和用户的合法性。智能决策机制利用历史数据训练机器学习模型，实现实时推理和决策，自动或半自动地执行相应操作，结果表明，战略和机制能有效提高边缘计算环境的安全性和效率，为各种工业和商业场景提供强大的安全保障。

关键词：边缘计算；网络安全；智能决策

引言：

边缘计算作为一种新兴的计算模式，正逐渐改变着数据处理和服务的格局。它将计算和数据存储从中心化的数据中心推向网络的边缘，近距离地为用户提供高效、低延时的服务。由于边缘设备通常分布在广泛的地理区域，且往往缺乏足够的物理和逻辑安全措施，这使得它们更容易受到攻击。因此，需要设计并实施一套针对边缘计算环境的网络安全策略，以保护数据的安全性和隐私性。

1 边缘计算环境下的网络安全问题

1.1 边缘计算环境概述

边缘计算收集并分析数据的行为发生在靠近数据生成的本地设备和网络架构中，而并非将数据传输至计算资源集中化的云端进行数据处理[1]。将部分数据分析功能，放到了应用场景的附近（终端或网关）来实现。

1.2 网络安全问题分析

第一，在数字化时代，数据已经成为一种新的资产，然而，它也是网络攻击者的主要目标。企业和个人的敏感信息，如财务记录、身份信息、登录凭证等，在未经授权的情况下被访问、披露、修改或销毁的风险持续上升；第二，技术进步使网络攻击更复杂隐蔽，如钓鱼、勒索软件、DDoS 和利用零日漏洞等攻击。这些攻击不仅可能导致系统瘫痪，还可能窃取数据、金融欺诈或破坏关键设施。物联网普及带来便利，也带来新安全挑战。设备缺乏强大防护且常被忽视在安全策略外，易成攻击者入口。攻击者可入侵物联网设备获取敏感信息、进行中间人攻击或发动更大规模网络攻击。

2 网络安全策略

2.1 访问控制策略

从边缘计算环境下的网络架构特点出发，企业和组织必须实施严格的访问控制机制，以防止未经授权的用户访问敏感信息[2]。网络安全需建立访问权限体系，为每个用户或用户组分配适当的访问级别和权限，确保用户只能访问完成任务所需的最小数据集。实施最小权限原则，并随着员工职位变化定期审查和调整网络安全及访问权限。例如，财务人员只能访问财务记录，不能访问研发部门的机密文档。高级别用户组（财务人员、研发人员、人力资源）实施了手机验证、动态令牌和生物识别等额外身份验证步骤，以限制其访问敏感数据集。中级别用户组（市场部门和客户服务）采取较宽松策略，市场部门无额外验证，可能增加数据泄露风险。初级或受限访问用户组（实习生和外部合作伙伴）访问权限仅限于非核心数据集，并可采用生物识别、动态令牌或手机验证等额外验证步骤确保数据安全。

2.2 数据加密策略

在边缘计算环境中，由于其融合了以授权实体为信任中心的多信任域共存的计算模式，传统的数据加密和共享策略不再适用，基于多授权方的轻量级数据加密与细粒度数据共享成为新需求。将条件代理重加密 CPRE 与属性加密 ABE 相结合，提出一种基于密文策略的属性条件代理重加密方案，并通过 CPRE 中代理权限控制特性，完成高效的边缘计算[3]。本方案系统初始化算法生成公共参数和主密钥。属性授权算法为各属性授权机构生成公私钥对，确保其能管理和控制属性，且遵循严格安全标准。密钥生成算法根据用户属性集合生成私钥，从代理者到委托者的条件代理重加密密钥，使代理者可在满足条件下重新加密并转发密文，提高系统灵活性和效率。

2.3 身份认证策略

边缘计算的设备和传统中心化的服务器不同，它们往往部署在易受攻击的环境中，例如在公共场所。因此，识别这些设备的潜在风险，如物理接入或未经授权的远程访问是至关重要的。定期进行设备的安全审查和风险评估[4]。为了应对边缘计算中的安全挑战，需要对不同的用户进行身份验证，并对访问权限进行严格控制。边缘计算设备部署在多样化的环境中，从公共场所到工厂车间，每个环境都带来了特定的潜在风险。

3 智能决策机制

3.1 基于机器学习的智能决策背景

就目前的网络防御手段而言，大体逃不过两种方式，一是在软件开发阶段引入各种规范，加强系统的安全性，减少攻击面；二是通过纵深防御的方式在网络的各个层面加强安全性，但是现在这种静态的防御手段已经不能满足日益复杂的网络环境[5]。

3.2 技术实施方案

当新的数据从终端设备或边缘设备传入时，机器学习模型会进行实时推理，为操作提供智能决策。基于历史数据，训练了一个预测机器人手臂故障的模型。根据机器学习模型的推理结果，边缘计算中基于机器学习的智能决策流程见表 4。

表 4　边缘计算中基于机器学习的智能决策流程

阶段	数据来源	数据示例	处理/决策	结果/反馈
数据收集	机器人手臂传感器	位置：（x=10.5，y=20.3） 速度：5m/s 力度：80N 温度：45° C	–	–
实时推理	边缘服务器上的故障预测模型	输入：位置、速度、力度、温度等数据	预测未来 1 小时故障概率	预测故障概率：10%
决策执行	边缘计算系统	根据故障概率	降低手臂工作速度至 3m/s	速度已调整
			发送维护警报至工厂管理员	警报已发送
响应与反馈	工厂管理员	接收维护警报	进行手臂检查	发现手臂轴承磨损
		执行必要维护操作	更换手臂轴承	手臂轴承已更换
数据（反馈循环）	机器人手臂状态监测	状态：维护完成，运行正常	更新故障预测模型	故障预测模型已更新

由于预测到机器人手臂可能发生故障，系统自动降低了该手臂的工作速度并发送了维护警报给工厂管理员。工厂管理员收到警报后进行了检查，并确认手臂确实存在问题。他进行了必要的维护，并将结果反馈给了系统。基于机器学习的智能决策机制在边缘计算环境中具有巨大的潜力。它可以实时处理和分析数据，提供准确的预测和决策，从而优化操作、预防故障并提高整体效率。

结论

本文提出的访问控制、数据加密和身份认证等策略，为边缘计算环境构筑了坚固的安全防线。通过严格的访问控制，确保只有经过授权的用户才能访问到敏感数据，从而避免了数据泄露的风险。基于多授权方的轻量级数据加密方案，不仅保证了数据在传输和存储过程中的机密性，还降低了加密操作对系统性能的影响。

参考文献：

[1]杜璞.移动边缘计算环境下 5G 通信网络数据安全与隐私保护技术研究[J].长江信息通信，2022，35（10）：211-214.

[2]李晓伟，陈本辉，杨邓奇，等.边缘计算环境下安全协议综述[J].计算机研究与发展，2022（059-004）.

[3]李云，高倩，姚枝秀，等.移动边缘计算中智能服务编排和算网资源分配联合优化方法[J].通信学报，2023，44（7）：51-63.

[4]朱宏颖，张新有，邢焕来，et al.边缘计算环境下轻量级终端跨域认证协议[J].网络与信息安全学报，2023，9（4）：74-89.

[5]杜翠凤邹光健.边缘计算环境下网络拓扑拟态关联图与主动防御模型研究[J].广东通信技术，2022，42（8）：62-66.