广播电视网络安全运维保障服务平台的构建

谢 徵

（山西广播电视台 太原 030001）

摘 要 广播电视媒体不仅是信息传播的工具，更是传播文化和引导社会舆论的关键载体。然而，网络攻击、数据泄露、信息篡改等安全事件层出不穷，对广播电视网络系统的正常运行构成了严重威胁。文中从广播电视网络安全运维保障服务平台的概念出发，分析了该平台的设计思路，希望能为从业者提供有效的参考。

关键词： 广播电视；网络安全；服务平台

中图分类号 TP311.5

Construction of Broadcasting and Television Network Security Operation and Maintenance Guarantee Service Platform

XIE Zheng

（Shanxi Radio and Television Station，Taiyuan 030001，China）

Abstract Radio and television media is not only a tool for information dissemination, but also a key carrier for disseminating culture and guiding public opinion. However, security incidents such as network attacks, data leakage, and information tampering continue to emerge, posing a serious threat to the normal operation of radio and television network systems. Starting from the concept of radio and television cyber security operation and maintenance support service platform, this paper analyzes the design ideas of the platform, hoping to provide effective reference for practitioners.

Key words Radio and television，Network security，Service platform

0 引言

随着信息技术的快速发展，广播电视系统的网络安全问题越来越复杂。为有效应对日益增长的网络安全威胁，需要构建一个综合性的广播电视网络安全运维保障服务平台[1]。本文探讨了该平台的设计思路和技术架构，旨在为广播电视行业提供一种切实可行的解决方案。

1 相关概述

广播电视网络安全运维保障服务平台是一种综合性的技术体系，旨在为广播电视网络的安全运行提供全方位的支持与保障。该平台通常可以采用分层架构，分为用户层、本地服务层、云端服务层3个层次，如图1所示。

（1）用户层主要面向各类用户终端设备，包括电视机、机顶盒、移动设备等。该层负责采集用户的使用数据、行为日志及设备状态，提供必要的安全警示能力和用户交互功能，实现对用户端安全状况的实时监控和快速响应。

（2）本地服务层则集中在广播电视网络的各个节点上，包括机房、基站、数据中心等关键基础设施。该层主要负责数据的初步处理和存储，以运行各种安全防护措施，如防火墙、入侵检测系统、防病毒软件等。此外，本地服务层还负责设备的日常维护和故障排除，确保网络基础设施的稳定运行。

（3）云端服务层是平台的核心部分，具有大数据分析、人工智能算法和集中管理功能。通过实时汇总和分析来自用户层和本地服务层的数据，云端服务层可以识别潜在的安全威胁，并采取相应的防护措施。该层还具备强大的计算和存储能力，能处理海量数据，支持广泛的安全策略和应急预案[2]。此外，云端服务层可提供统一的管理界面和报告功能，以便运维人员进行集中管理和决策支持。

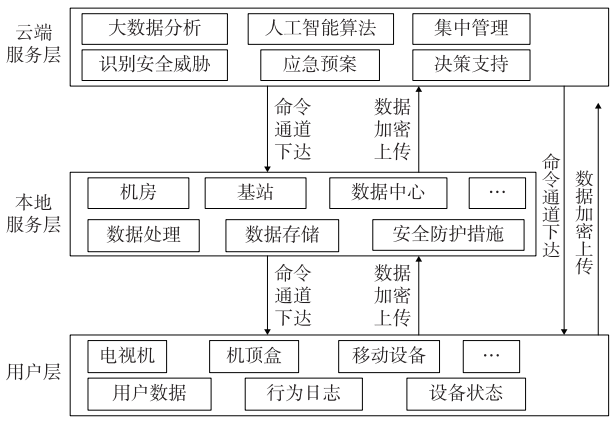

图1 平台整体架构

作者简介：谢徵（1987—），硕士，工程师，研究方向为网络数据安全。

2 平台设计思路

2.1 综合防护

在高度互联的数字时代，广播电视网络面临着前所未有的安全挑战。为确保广播电视网络的稳定运行和信息安全，采用综合性的防护措施尤为重要。综合防护不仅是对单一环节的保护，还是对整个系统的多层次、多维度防护。因此，需要引入先进的威胁情报和态势感知技术，实时监测网络中的异常行为。例如，部署网络入侵检测系统（IDS）和网络入侵防御系统（IPS），可以及时发现并阻止潜在的攻击行为。引入人工智能和机器学习技术，可以提升威胁识别的准确性和响应速度。

由于广播电视网络传输的大量数据中包含敏感信息，如果这些敏感信息被不法分子窃取或篡改，则可能会导致严重的后果。为应对这些潜在的威胁，除使用传统的防护手段外，还需要考虑数据的加密和访问控制。使用强大的加密算法，可以确保数据在传输过程中无法被轻易拦截和解密。此外，终端设备是广播电视网络的重要组成，也是最容易被攻击者利用的薄弱点。应用端点检测与响应（Endpoint Detection and Response，EDR）技术，可以对终端设备进行实时监控和防护。EDR技术能在终端设备上检测并响应潜在的威胁，快速隔离受感染的设备，防止攻击扩散，并提供详细的事件分析和溯源功能。此外，还需要定期进行安全培训，提高工作人员的安全意识，防止因人为疏忽造成的安全风险。

2.2 智能监控

通过智能监控，可以实时掌握广播电视网络安全运维保障服务平台网络的运行状态，及时发现并处理潜在的安全威胁，确保网络的稳定性和安全性。因此，需要建立一个全面的监控体系，覆盖广播电视网络的各个层面。该监控体系不仅包括传统的网络设备，如路由器、交换机、防火墙等，还包括服务器、存储设备和各类终端设备。通过部署网络监控系统（NMS），可以实时收集和分析各类设备的运行数据，及时发现异常情况。

智能监控需要引入大数据分析和人工智能技术，通过对海量监控数据的分析，发现潜在的安全威胁和网络故障。例如，利用机器学习算法，可以分析网络流量，识别异常的流量模式，提前预警可能的攻击行为。通过态势感知技术，可以实时监控全网的安全态势，及时发现和处置安全事件。同时，引入自动化的运维工具，可以在发现安全威胁或网络故障时自动执行预定义的应急响应措施[3]。例如，当检测到网络攻击时，可以自动启动防火墙，封锁攻击源IP地址；发现服务器异常时，可以自动触发故障转移机制，确保业务的连续性。

2.3 快速响应

在面对广播电视网络突发安全事件时，快速响应能力不仅可以最大限度地减少损失，还能在短时间内恢复正常的服务，确保广播电视网络的稳定性和连续性。因此，需要建立完善的应急响应机制，制定详细的应急预案，明确各类安全事件的处置流程和责任分工，确保相关人员能在发生安全事件时迅速行动。定期进行应急演练，检验应急预案的有效性，发现并改进存在的问题，提升应急响应能力。

此外，需要组建一支专业的安全应急响应团队（CSIRT），负责全网的安全事件处置工作。快速响应团队应具备丰富的网络安全知识和实战经验，能在第一时间发现和分析安全事件，制定并实施应对措施。团队成员需保持高度警惕，时刻关注网络安全态势，以便在发生安全事件时迅速响应。此外，快速响应还需要借助自动化的工具和平台。通过部署安全事件管理平台（SIEM），可以实现安全事件的集中管理和快速处置。利用自动化工具，可以实现安全事件的实时监控、自动告警和快速处置，减少人工干预，提高响应效率。

3 平台构建

3.1 数据采集层构建

数据采集层是整个平台的基础，其主要任务是从网络的各个设备和节点获取相关数据，为后续的分析和处理提供基础。该层可通过部署分布式的数据采集代理，实时收集来自这些设备的日志、流量、性能指标和告警信息。因此，可以采用分布式架构，保证其高可用性和扩展性，确保其能在大规模网络中高效运行。在数据采集过程中，由于广播电视网络中存在多种类型的设备和数据源，包括网络设备、服务器、存储设备、终端设备等，可通过多源数据融合技术对不同来源的数据进行统一处理和分析，提高数据的全面性和可靠性。

为确保安全运维平台能及时响应和处理安全事件，必须保证数据传输路径的畅通性。可以采用高速网络和优化的数据传输协议，确保数据传输的低延迟和高可靠性。在数据传输过程中，需要考虑网络环境的复杂性，保证不同网络条件下的数据传输质量。在数据传输和存储过程中，需要确保数据的安全性。此外，可以采用分布式存储系统，保证数据存储的可靠性和可扩展性。在数据管理方面，需要建立完善的数据索引和检索机制，确保数据查询和利用的高效性。

3.2 数据处理层构建

数据处理层可以清洗、转换和分析采集到的大量原始数据，以提取有价值的信息，便于后续的决策和响应。为实现该目标，数据处理层需要具备强大的数据处理能力和灵活的扩展性。因此，可以采用Hadoop和Spark大数据处理平台技术，以高效地处理和分析海量数据。这些平台支持分布式的计算和存储，使得数据处理和分析能在多个节点上并行进行，提高了处理效率和系统的可扩展性，具体过程

如图2所示。

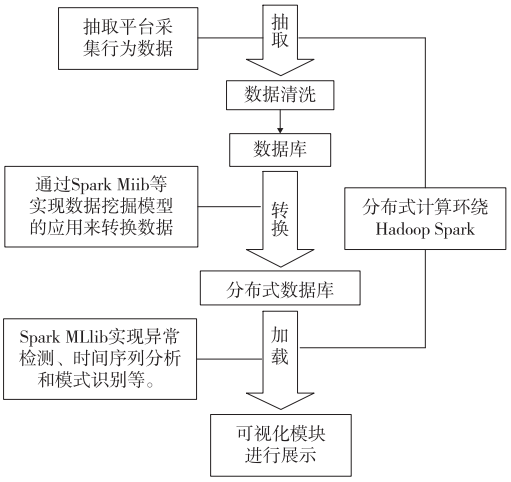

图2　基于Hadoop和Spark的数据处理过程

（1）数据清洗模块负责对原始数据进行预处理，包括数据格式转换、缺失值填补、冗余数据删除等，保证数据分析的质量。（2）转换模块可通过Spark Miib等，应用数据挖掘模型来转换数据。Spark MLlib提供了一系列强大的机器学习算法和工具，能轻松地对数据进行分类、回归、聚类等操作，从中提取出有价值的信息。（3）分布式数据库可以高效地存储经过转换的数据，快速响应查询请求，确保数据的可用性和低延迟。（4）分析模块负责深度分析经过清洗和转换的数据，从中发现潜在的安全威胁和异常行为。该模块同样依赖于Spark MLlib提供的高级分析算法，如异常检测、时间序列分析和模式识别。（5）可视化模块可以展示分析结果，利用数据可视化技术（如D3.js和Tableau），将复杂的数据分析结果转化为直观的图表和仪表盘。通过这些可视化工具，运维人员能快速理解数据中的关键信息，并据此作出及时和有效的响应。

3.3　平台安全层构建

平台安全层主要负责保护数据的机密性、完整性和可用性，可通过多层次的安全机制来防范各种潜在的安全威胁和攻击。为实现该目标，可以采用OAuth2.0认证框架来管理用户身份和权限，确保只有授权用户才能访问敏感数据和系统功能。OAuth2.0框架不仅支持多种认证方式，如密码认证、授权码认证和客户端凭证认证，还能与其他安全机制如双因素认证（2FA）结合使用，进一步提高系统的安全性。该框架主要包含用户界面模块、服务模块、数据模块和RBAC权限管理模块，如图3所示。其中，用户界面模块主要负责用户身份验证的交互界面，确保用户能方便地进行登录和权限管理操作。服务模块负责处理身份验证服务、授权服务和安全管理服务请求。数据模块则负责存储和管理用户身份信息、权限配置信息以及审计日志，确保敏感数据的安全存储和高效访问。RBAC权限管理模块则基于角色进行权限分配，确保不同角色的用户只能访问其所需的功能和数据，减少权限滥用的风险。

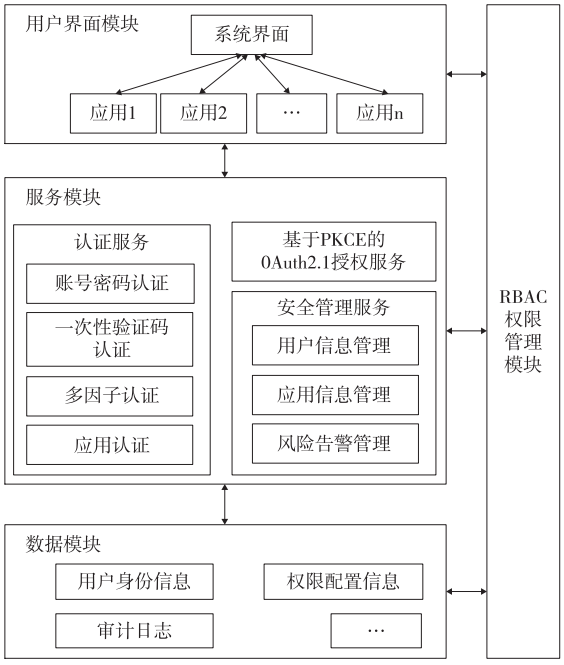

图3　OAuth2.0框架认证方式

为进一步提升平台的安全性，还可以引入加密技术和安全协议。所有敏感数据在传输和存储过程中都应进行加密处理，确保数据在传输过程中无法被窃取或篡改。可以采用传输层安全协议（TLS）来保护数据传输的安全性，确保数据传输的机密性和完整性。此外，需要定期进行安全审计和漏洞扫描，及时发现并修复系统中的安全漏洞，防范潜在的攻击风险。

4　结语

广播电视网络安全运维保障服务平台的设计与构建需要综合考虑多层次、多维度的防护措施。通过引入先进的威胁情报和态势感知技术、智能监控及快速响应机制，可以有效提升整个系统的安全性和稳定性。在数据处理层的构建中，采用Hadoop和Spark等大数据处理平台技术，不仅能高效处理海量数据，还能通过数据清洗、转换和深度分析，从数据中提取有价值的信息，支持决策和响应。平台安全层则通过OAuth2.0认证框架和多层次的安全机制来确保数据的机密性、完整性和可用性。未来，随着技术的不断发展，该平台将不断升级和完善，进一步提高广播电视行业的安全性。

参考文献

[1] 汪巍，陈玖根，陈玉芬.广电网络工业互联网的安全公共服务平台分析[J].声屏世界，2023(18)：93-95.

[2] 王佳君.基于“云计算”虚拟化技术高校计算机网络安全实训实验室构建分析[J].信息技术与信息化，2021(11)：222-224.

[3] 吴双林，程志伟，李玥.互联网技术下影像云服务平台的应用与实践[J].网络空间安全，2022，13(2)：61-66.