基于云计算的网络安全隐私数据融合探讨

郑利武　杨　鑫*
深信服科技股份有限公司杭州分公司　浙江杭州　310000

摘　要：近年来，危险驾驶冲撞人群事件频发，严重威胁公共安全，对社会秩序和公民生命财产安全造成极大危害。本文以危险驾驶冲撞人群事件为例，探讨以危险方法危害公共安全行为的预警与处置策略。通过分析数据融合技术在公共安全领域的应用，提出基于云计算的网络安全隐私数据融合框架，旨在提高预警系统的实时性和准确性。研究首先概述数据融合技术的定义、分类及隐私保护问题；其次，设计一个云计算环境下的数据融合框架，详细阐述其架构模型、数据融合流程及安全保护技术；随后，分析当前网络安全隐私数据融合中存在的大规模数据安全与隐私性、云环境下数据隔离与整合、计算效率与性能等问题；最后，提出强化数据加密与访问控制机制、使用分布式计算与边缘计算优化数据融合过程、实现差分隐私和多方安全计算结合等解决方案。本研究为公共安全事件的预警与处置提供了理论支持和技术参考，有助于提升应对危险驾驶冲撞人群等突发公共安全事件的能力。

关键词：云计算；网络安全隐私；数据加密；数据融合

公共安全是社会稳定和发展的基石，而危险驾驶冲撞人群事件作为一种典型的以危险方法危害公共安全行为，其突发性和危害性引起了广泛关注。这类事件不仅造成人员伤亡和财产损失，还对社会心理产生深远影响。传统的公共安全预警与处置方法往往存在信息孤岛、响应滞后等问题，难以有效应对日益复杂的公共安全威胁。随着信息技术的发展，数据融合技术为公共安全预警提供了新的思路。通过整合多源异构数据，数据融合技术能够提高预警的准确性和实时性。然而，数据融合过程中的隐私保护和网络安全问题也不容忽视。本文旨在探讨如何利用数据融合技术，特别是基于云计算的数据融合框架，构建高效、安全的公共安全预警系统，并以危险驾驶冲撞人群事件为例，分析预警与处置的关键技术和策略，为公共安全管理提供理论和技术支持。

一、数据融合技术概述

（一）数据融合的定义与分类

随着云计算技术的快速发展，越来越多的企业和个人开始依赖云计算平台进行数据存储和计算服务，云计算的优势在于其动态可扩展性和高可靠性，能够满足不同规模用户的需求，同时提供低成本的解决方案，使得企业和个人能够在不增加大量硬件投资的情况下，享受到高效的网络服务[1]。然而，随着用户数量的急剧增加，云计算平台面临着数据安全和隐私保护的严峻挑战。传统的静态存储模式已无法满足大规模数据系统的需求，尤其是在数据存储和传输过程中，可能存在认证权限不足或数据验证漏洞的风险[2]。例如，下载到本地文件夹存储的数据，往往无法有效保障其完整性和安全性，这使得数据容易受到未经授权的访问或篡改，进而影响企业和个人的数据隐私。随着云计算技术的不断发展，动态数据追踪与处理成为提升数据安全性的重要手段，通过云平台的共享访问机制，用户可以根据不同的使用特征和需求进行权限配置和管理[3]。然而，为了确保数据的私密性和安全性，必须设置严格的用户权限过滤和隔离保护机制[4]。这些机制能够有效避免敏感信息的泄露，并确保在不同用户之间进行合理的数据隔离。同时，权限维护是实现数据安全的重要环节，定期更新和管理用户的访问权限，可以最大程度降低潜在的安全风险。在硬件设施方面，云计算减少了用户在本地服务器上的投入，通过虚拟化技术实现更高效的资源利用。结合产业和信息技术的发展，云计算不仅推动了信息技术的创新应用，也促进了各行业之间的协同发展。通过高度集成的技术架构，各行业能够共享核心数据信息，提升决策效率，并进一步推动产业的转型升级[5]。

根据处理层次的不同，数据融合可以分为三类，其

作者简介：
郑利武（1988.8-），男，汉族，广东揭阳人，本科，研究方向为网络安全和数据安全方向。
杨鑫（1994.9-），男，汉族，湖北十堰人，硕士研究生，研究方向为网络安全和数据安全方向。

中，数据级融合是最底层的融合，直接对原始数据进行整合和处理，适用于数据同质性较高的场景；特征级融合则是对提取的特征进行融合，适用于数据异质性较高的场景；决策级融合是最高层次的融合，基于各独立决策结果进行综合判断，适用于复杂决策场景。在公共安全领域，数据融合技术可以整合视频监控、社交媒体、传感器网络等多源数据，为危险驾驶冲撞人群等突发事件的预警和处置提供全面、实时的信息支持。

（二）数据融合中的隐私保护

数据融合技术在提高信息处理能力的同时，也带来了隐私保护的挑战。隐私保护的核心在于确保个人敏感信息在数据融合过程中不被泄露或滥用。常见的数据融合隐私保护技术包括数据匿名化、数据加密和访问控制等。数据匿名化通过去除或模糊数据中的个人标识信息，降低数据被关联到具体个体的风险；数据加密则通过密码学技术确保数据在传输和存储过程中的安全性；访问控制通过权限管理限制数据的使用范围和人员。在公共安全领域，隐私保护尤为重要，因为公共安全数据往往涉及大量个人隐私信息。如何在确保数据融合效果的同时保护个人隐私，是数据融合技术应用中需要解决的关键问题。例如，在危险驾驶冲撞人群事件的预警中，视频监控数据可能包含行人面部信息，需要通过技术手段确保这些信息不被滥用。

二、基于云计算的网络安全隐私数据融合框架

（一）框架设计与架构模型

基于云计算的网络安全隐私数据融合框架旨在提供一个高效、安全的数据处理平台，以支持公共安全事件的预警与处置。该框架采用分层架构模型，包括数据采集层、数据传输层、数据融合层和应用层。数据采集层负责从多源异构数据源（如视频监控、社交媒体、传感器网络等）收集原始数据；数据传输层通过加密通道确保数据在传输过程中的安全性；数据融合层是框架的核心，通过云计算平台实现数据的整合、分析和处理；应用层则提供预警、决策支持等具体功能。该框架的关键在于利用云计算的弹性计算和存储资源，实现大规模数据的高效处理，同时通过隐私保护技术确保数据的安全性。例如，在危险驾驶冲撞人群事件的预警中，该框架可以实时整合交通监控和社交媒体数据，快速识别潜在威胁并触发预警机制。

（二）数据融合流程与算法分析

数据融合流程包括数据预处理、特征提取、数据融合和结果输出四个主要步骤。数据预处理阶段对原始数据进行清洗、去噪和标准化，以提高数据质量；特征提取阶段从预处理后的数据中提取关键特征，如车辆速度、行驶轨迹等；数据融合阶段通过算法将多源特征进行整合，生成综合判断；结果输出阶段将融合结果转化为预警或决策支持信息。常用的数据融合算法包括卡尔曼滤波、贝叶斯网络、D–S证据理论等。卡尔曼滤波适用于动态数据的实时融合；贝叶斯网络能够处理不确定性和概率推理；D–S证据理论则适用于多源信息的综合判断。在云计算环境下，这些算法可以通过并行计算和分布式处理实现高效运行，满足公共安全事件对实时性的要求。

（三）数据安全与隐私保护技术

在基于云计算的数据融合框架中，数据安全与隐私保护技术是确保系统可靠性和合规性的关键。常用的技术包括同态加密、安全多方计算和差分隐私等。同态加密允许在加密数据上直接进行计算，而无需解密，从而保护数据隐私；安全多方计算允许多方在不泄露各自私有数据的情况下进行联合计算；差分隐私则通过添加噪声确保个体数据不被识别。此外，访问控制机制和身份认证技术也是框架的重要组成部分，用于限制数据的访问权限和使用范围。在危险驾驶冲撞人群事件的预警中，这些技术可以确保敏感数据（如行人身份信息）在融合过程中不被泄露，同时满足公共安全管理的需求。

三、网络安全隐私数据融合中存在的问题

（一）大规模数据的安全性与隐私性问题

随着公共安全数据的爆炸式增长，大规模数据的安全性与隐私性问题日益突出。数据融合过程中，多源数据的整合增加了数据泄露的风险，尤其是在云计算环境下，数据的集中存储和处理使得其成为攻击的主要目标。此外，不同数据源的安全标准和隐私保护水平不一，可能导致安全短板效应。例如，社交媒体数据可能缺乏严格的隐私保护措施，而视频监控数据则可能包含高度敏感的个人信息。如何在数据融合过程中确保所有数据的安全性和隐私性，是一个亟待解决的问题。

（二）云环境下的数据隔离与整合问题

云计算环境下的数据隔离与整合问题也是数据融合技术面临的重要挑战。一方面，多租户环境下，不同用户或应用的数据需要严格隔离，以防止数据交叉访问和泄露；另一方面，数据融合又要求打破数据孤岛，实现跨源、跨域的数据整合。这种矛盾使得数据隔离与整合成为技术难点。例如，在危险驾驶冲撞人群事件的预警中，交通管理部门和公安部门的数据可能需要共享和融合，但又必须确保各自数据的独立性和安全性。当前的

解决方案往往需要在安全性和融合效果之间进行权衡，难以同时满足两者需求。

（三）计算效率与性能问题

数据融合的计算效率与性能问题在公共安全应用中尤为重要，因为预警和处置往往对实时性要求极高。云计算环境虽然提供了强大的计算能力，但数据融合过程中的复杂算法和大规模数据处理仍可能导致延迟。例如，实时视频分析和高维数据融合需要大量的计算资源，可能超出云平台的即时处理能力。此外，隐私保护技术的引入（如同态加密和安全多方计算）也会显著增加计算开销，进一步影响系统性能。如何在确保隐私和安全的前提下，提高数据融合的计算效率，是当前研究的热点问题。

四、解决方案与策略

（一）强化数据加密与访问控制机制

针对大规模数据的安全性与隐私性问题，强化数据加密与访问控制机制是关键，采用先进的加密技术，如AES和RSA算法，可以实现对数据的端到端加密，确保数据在传输和存储过程中的高度安全性，并通过加密保护可以数据在整个过程中避免了未经授权的访问和潜在的安全风险，有效提升了信息安全性。其次，实施细粒度的访问控制策略，基于角色或属性的访问控制（RBAC/ABAC）可以有效限制数据的访问权限，防止未授权访问。定期进行安全审计和漏洞扫描是确保系统安全的关键步骤，有助于及时发现并修复潜在的安全隐患。尤其在危险驾驶冲撞人群事件的预警系统中，采用加密技术保护视频监控数据的安全性，防止数据泄露和滥用。同时，实施严格的访问控制措施，确保只有经过授权的人员可以访问和处理敏感信息，从而有效保障系统的整体安全性，提升对突发事件的应对能力。

（二）使用分布式计算与边缘计算优化数据融合过程

为提高计算效率与性能，可以采用分布式计算与边缘计算技术优化数据融合过程。分布式计算通过将任务分解到多个计算节点并行处理，显著提高处理速度；边缘计算则将部分计算任务下沉到数据源附近，减少数据传输延迟和带宽消耗。例如，在危险驾驶冲撞人群事件的预警中，可以在交通监控摄像头端进行初步的视频分析（如车辆速度检测），仅将关键特征数据传输到云端进行进一步融合，从而降低云平台的计算负担和响应时间。

（三）实现差分隐私和多方安全计算的结合

为解决云环境下的数据隔离与整合问题，可以结合差分隐私和多方安全计算技术，差分隐私通过添加噪声保护个体数据隐私，适用于数据发布和共享场景；多方安全计算则允许多方在不泄露各自私有数据的情况下进行联合计算，适用于数据融合场景。两者的结合可以在保护隐私的同时实现高效的数据整合。例如，在跨部门数据融合中，交通部门和公安部门可以通过多方安全计算共享数据特征，而无需暴露原始数据，同时通过差分隐私确保共享结果不会泄露个体信息。

结语

综上所述，本文以危险驾驶冲撞人群事件为例，探讨了以危险方法危害公共安全行为的预警与处置策略，重点研究了数据融合技术在公共安全领域的应用。通过构建基于云计算的网络安全隐私数据融合框架，分析了数据融合的定义、分类、隐私保护技术以及框架的设计与实现。同时，指出了当前数据融合中存在的大规模数据安全与隐私性、云环境下数据隔离与整合、计算效率与性能等问题，并提出了强化数据加密与访问控制、使用分布式计算与边缘计算、结合差分隐私和多方安全计算等解决方案。这些研究为公共安全事件的预警与处置提供了理论支持和技术参考，有助于提升应对危险驾驶冲撞人群等突发公共安全事件的能力。未来，随着技术的进一步发展，数据融合技术将在公共安全领域发挥更加重要的作用，为构建安全、智能的社会提供有力支撑。

参考文献

[1]傅江辉.基于云计算的社交网络安全隐私数据融合方法[J].济南大学学报（自然科学版），2021，35（1）：29-33.

[2]侯郭垒.大数据安全的立法保障研究[D].武汉：中南财经政法大学，2020.

[3]刘奕.5G网络技术对提升4G网络性能的研究[J].数码世界，2020（4）：24.

[4]杨修玮.基于数据挖掘的网络隐私数据防篡改方法研究[J].信息技术与信息化，2021（12）：112-114.

[5]李乃权.基于区块链的隐私数据安全综述[J].网络安全技术与应用，2022（1）：19-21.