

跨域访问控制技术研究

诸天逸^{1,2}, 李凤华^{1,2}, 成林³, 郭云川^{1,2}

- (1. 中国科学院信息工程研究所, 北京 100195;
2. 中国科学院大学网络空间安全学院, 北京 100049;
3. 中国信息安全测评中心, 北京 100085)

摘要: 根据国内外最新研究, 对跨域数据流动中的访问控制技术进行了总结和展望。首先, 结合复杂应用环境下的访问控制, 概括了访问控制模型、数据安全模型的发展。其次, 分别从数据标记、策略匹配和策略冲突检测方面对访问控制策略管理的研究展开论述。最后, 总结归纳了统一授权管理中数据标记技术和授权与延伸控制技术的研究现状。

关键词: 跨域数据流动; 访问控制模型; 策略授权管理

中图分类号: TN 929

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021003

Research on cross-domain access control technology

ZHU Tianyi^{1,2}, LI Fenghua^{1,2}, CHENG Lin³, GUO Yunchuan^{1,2}

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. China Information Technology Security Evaluation Center, Beijing 100085, China

Abstract: Based on the latest research at home and abroad, the access control technology in cross-domain data flow were summarized and prospected. Firstly, combined with access control in complex application environments, the development of access control models and data security models were summarized. The advantages and disadvantages of access control policy management were analyzed. Secondly, the research on access control policy management from the aspects of data marking, policy matching and policy conflict detection were discussed respectively. Finally, the research status of data marking technology and authorization and extension control technology in unified authorization management were summarized.

Keywords: cross-domain data flow, access control model, policy authorization management

收稿日期: 2020-05-08; 修回日期: 2020-07-21

通信作者: 诸天逸, zhutianyi@iie.ac.cn

基金项目: 国家重点研发计划(2016QY06X1203); 国家自然科学基金(U1836203); 山东省重点研发计划(重大科技创新工程)(2019JZZY020127)

Foundation Items: The National Key Research and Development Program of China (2016QY06X1203), The National Natural Science Foundation of China (U1836203), Shandong Provincial Key Research and Development Program (2019JZZY020127)

论文引用格式: 诸天逸, 李凤华, 成林, 等. 跨域访问控制技术研究[J]. 网络与信息安全学报, 2021, 7(1): 20-27.

ZHU T Y, LI F H, CHENG L, et al. Research on cross-domain access control technology[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 20-27.

1 引言

随着网络与信息技术的持续快速发展,不同的政府部门、企事业单位均建设有若干不同的业务信息系统。由于受控对象和业务场景的不同、客观实际应用中管理模式的不同,这些业务系统呈现域内互联、域间孤立特征,使现实应用中各个业务系统的数据未被充分利用,这与系统互联的信息传播与共享协同本质相悖。在此背景下,一些管理部门要求打破不同管理域、不同安全域、不同业务系统间的数据流动壁垒,建立统一的数据中心来存储不同管理域、不同安全域、不同业务系统所产生的海量异构数据,在确保数据细粒度受控使用的前提下,实现所有被授权的数据使用者能依据自身需求在任何时间、任何地点,使用任意终端设备、通过任意渠道接入任何网络依规获取跨管理域、跨安全域、跨业务系统的数据。

毫无疑问,跨管理域、跨安全域、跨系统数据流动的服务模式必将大幅提升业务部门的处理效率。然而,这种服务模式要求将现有孤立系统进行物理连接和逻辑隔离,势必打破原有信息系统在管理上数据隔离的信息孤岛现状;同时跨管理域、跨安全域的信息系统在业务服务、安全管理等方面存在差异,敏感数据会在不同信息系统中存留,产生了新的访问控制问题:如何确保跨区域的数据访问者只有在受控模式下才能获得完成业务功能所必需的数据,并确保所获取的数据不被非授权传播。

跨管理域、跨安全域、跨业务互联系统所产生的数据来自不同的机构、组织与个人,具有多源特征;不同数据源持续生成大量的数据,呈现海量特征;这些海量数据类型包含多媒体数据、业务数据、管理数据等,缺乏统一的格式与规范,具有明显的半结构化和非结构化特征。上述特征直接导致了数据使用在授权与鉴权方面面临两个挑战。

1) 信息控制模式:由于计算成本、存储成本和维护成本等约束,单个机构难以独自建立数据中心,因此,各个机构不得不将数据存储到第三方管理的数据中心,使数据所有权和管理权分离,直接导致了信息控制模式有别于传统的访问控

制,即传统访问控制中数据所有权和管理权属于同一机构或个人,数据所有者信任数据管理者,而管理数据中心的第三方是半可信甚至不可信的。

2) 细粒度访问授权与延伸控制:首先,由于各种不同数据在安全保护等级、知悉范围和管理者利益等方面存在差异,来自不同管理域、不同安全域、不同信息系统的数据不能完全无条件共享,需在约束条件下进行受控共享,而实践过程中约束条件缺乏清晰准确的定义,且访问权限随访问者访问时间、地点和所使用设备等环境动态变化。其次,现有访问控制系统中访问控制主体/客体数量有限,且属性定义单一,使数据访问过程中细粒度控制困难。此外,现有访问控制系统主要控制域内数据,一旦数据交换,数据复制的所有者就可能对数据进行任意传播,从而导致传播失控。

针对上述问题,学术界和产业界展开了广泛的研究,本文从复杂应用环境下的访问控制模型与数据访问安全模型、访问控制策略管理、统一授权与延伸控制等角度梳理跨域访问控制研究现状,支撑用户跨域访问与数据跨域流动。

2 访问控制模型与安全模型

2.1 复杂应用环境下访问控制模型

20世纪70年代至今,随着IT技术发展和信息传播方式演化,访问控制技术经历了3个发展阶段:以单机数据共享为目的的主机访问控制(其代表性工作为BLP、Biba等模型)、以单域内部数据共享为目的面向组织形态的访问控制(其代表性工作为RBAC、UCON等模型)以及互联网、云计算、在线社交网络等新型复杂应用环境下的访问控制。下面讨论新型复杂应用环境下访问控制模型研究现状。

访问控制模型方面:新型复杂应用环境的访问控制模型主要包括基于属性的访问控制和基于关系的访问控制两类。基于属性的访问控制通过对主体、客体、权限和环境属性的统一建模,描述授权和访问控制约束;基于关系的访问控制通过用户间关系来控制对数据访问权限的分配。

基于属性的访问控制将时间^[1]、空间位置^[2]、

访问历史^[3]、运行上下文^[4]等要素作为访问主体、访问客体和环境的属性来控制数据访问行为,通过定义属性间的关系来描述复杂的授权和访问控制约束,确保授权的灵活性、匿名性与可靠性^[5-11],基于属性的访问控制的主要应用场景是云计算。基于关系的访问控制中,资源所有者将与访问者之间的关系(包括关系类型^[12]、关系强度^[13]等)作为控制要素,分配对数据的访问权限,确保隐私个性化保护和数据共享需求间的平衡,满足用户个性化、细粒度和灵活的授权要求,但基于关系的访问控制的主要应用场景是在线社交网络。

综上,目前新型应用环境下的访问控制模型主要聚焦于云计算和在线社交网络环境。但这些模型的本质仍是建模单域内数据控制,不适用于控制数据跨域流动;此外,这些模型未将多个要素进行融合控制,忽略了信息所有权和管理权分离等特征,不能直接建模跨管理域、跨安全域、跨业务系统的数据按需受控使用。笔者及所在团队在跨域受控共享访问控制模型方面取得了一些成果,即提出了基于行为的访问控制模型^[14]和面向网络空间的访问控制模型^[15],并从信息传播方式演进规律的角度预测了访问控制的未来发展趋势^[16-17]:资源访问请求者请求访问所需资源时,应考虑所处的时间状态、采用的终端设备、从何处接入、经由的网络/广义网络,以及要访问信息资源的安全属性等要素,确保“通过‘网络之网络’访问‘系统之系统’”的安全。这些工作为跨域受控共享访问控制建模提供了技术思路。

2.2 数据访问安全模型

针对数据访问中的核心操作及其操作规则的研究,目前学术界主要聚焦于以 BLP 为代表的信息流控制,确保数据不被直接或间接泄露。信息流控制的核心思想是:将标签附在数据上,并随着数据在整个系统中流动,限制数据流向。防止信息直接泄露的核心思想是准确执行“下读/上写”操作,防止间接泄露的核心概念是无干扰:确保系统在读/写执行过程中,受保护数据(高密级数据)与不受保护数据(低密级数据)间不相互干扰^[18-19]。

无干扰方面近期典型工作如下。Giacobazzi 等^[20]针对安全程序语言读/写原语所导致的数据

间接泄露问题,基于抽象无干扰概念,提出了弱信息流的统一检测框架,有效地提高了检测能力。Nielson 等^[21]针对内容依赖的信息流,提出了基于 Hoare 逻辑和内容依赖的信息流检测机制,采用指令操作语义证明所提出的 Hoare 逻辑的可靠性。Zhang 等^[22]针对三维干扰的数据传输方法,提出了一种基于蜂窝集群结构的干扰感知数据传输协议。笔者及所在团队^[23]针对结构化文档缺乏多级安全控制机制所产生的信息泄露问题,在 BLP 模型基础上对行为安全级别进行了细化,定义行为的读、写安全与基本的安全规则,采用无干扰理论证明其安全性。

综上,数据访问安全模型仅考虑读/写等操作及其规则,忽略了复杂应用环境下跨业务、管理、接入等系统中的其他操作与规则,不能满足数据访问安全性评估的需要。针对该问题,笔者及所在团队在前期研究中针对在线社交网络中的数据访问安全模型进行了初步研究,提出了 7 个原子操作^[24],这为构建数据访问安全模型提供了技术思路。

3 访问控制策略管理

访问控制策略管理主要聚焦于策略匹配、冲突检测与策略生成等方面的研究。

3.1 数据标记与策略生成

海量异构数据的细粒度自动标记是使用授权的基础,最早数据安全标记源自 BLP 模型,其安全标签包含密级和知悉范围。自 BLP 模型之后,国内外学者对数据标记展开了一系列研究,目前的研究主要聚焦于数据标签挖掘,包括标签补全、标签发现和标签排序等技术。

标签补全方面:针对 Web 文本中标签挖掘中的部分标签缺失问题,Yu 等^[25]提出了基于经验风险最小化的多标签学习技术,该技术可有效解决小规模数据集下标签缺失。针对智能传感数据中标签缺失问题,Cong 等^[26]提出了半监督的多任务学习模型(S2MTL),通过整合矩阵分解、映射特征词典、属性空间信息学习技术,大幅度提升属性补全效率。Guo 等^[27]提出了一种基于深度卷积神经网络(CNN)的标签完成和校正方法(LCC),并设计一种策略来补全标签并校正噪声

标记数据,使用完成和校正的结果不断修改模型以取得更好的效果。

标签发现方面:基于社交媒体中的众包数据,Yin等^[28]提出了面向地理空间视频的时空标签挖掘方案,该方案所挖掘的标签与用户直觉较为一致。Xu等^[29]提出了基于属性的访问控制策略挖掘方法,该方法通过合并和简化候选规则,可有效地改善挖掘效率。Yang等^[30]提出了跨媒体的标签迁移学习模型,该模型先创建了从图像到音频的知识转移渠道,提高了标签挖掘效率和准确度。基于异构网络,王瑜等^[31]提出了面向多标签系统的推荐模型,该模型将不同类型不可比较的标签映射到可比较的相同空间中,实现标签推荐优化。

标签排序方面:针对不同标签对数据描述影响重要性不同,Xin等^[32]提出了多标签分布式学习模型,提升了多标签挖掘的准确度和实用性。针对多模式图像检索(MIR)训练期间视觉和文本模态间不一致问题,Li等^[33]提出一种从图像文字描述中测量物体和场景标记重要性的方法,该方法能显著提升MIR性能。Wang等^[34]为无源标签提出了一种二维排序方法(HMO),通过观察标签的时间序列RSS变化,HMO可以获得标签的顺序以及特定的水平方向。

策略生成方面:吴迎红等^[35]提出了能描述策略间属性关联的精细化算法、记录策略和策略间关联属性的策略精细化树构建方法,为策略精细化中的策略关联问题处理提供基础;林莉等^[36]从规范策略合成和策略合成正确性目标出发,通过属性值的计算结构,建立了新的基于属性的策略合成代数模型。

目前,数据标签技术主要聚焦于挖掘单数据域单类型的标签,缺乏海量多源异构数据的归一化描述,需从分级标签自动融合、差异化数据按语义细粒度标记等方面展开研究,支撑海量异构数据的自动细粒度标记。

3.2 策略匹配

策略匹配方面:目前访问控制策略匹配主要聚焦于XACML策略匹配和XML策略匹配两类。

(1) XACML策略匹配研究主要包括3类:基于统计的策略顺序调整、策略缓存、高效策略匹配结构设计。基于统计的策略顺序调整首先对

策略/规则进行聚类,并依据策略访问频率对策略/规则类进行降序排列,确保优先匹配经常调用的策略^[37-38]。策略缓存机制将频繁调用的策略保存在高速单级或多级缓冲区中,避免从低速存储区进行重复检索^[37-39],并建立缓存索引,提高策略检索速度。上述两种方案未考虑嵌套层级等因素对策略匹配效率的影响,针对上述问题,学界提出了策略匹配结构设计方法,该方法采用决策图、决策树等数据结构对层级嵌套的策略/规则进行重新编排,并对数据类型进行转化;基于图/树结构,将策略匹配过程由顺序匹配变为树匹配或由二次匹配变为一次匹配,降低策略匹配复杂度^[40-42]。

(2) XML策略匹配研究主要包括3类:预处理、后处理和视图方式。预处理匹配发生在数据查询执行前,通过访问请求重写等方式将用户查询请求转化为被授权的安全请求,采用状态自动机等方式进行策略匹配,降低了访问请求的匹配时间^[43-44]。后处理方式发生在数据查询结果返回给用户前,先在数据库中执行用户的所有请求,再对非授权数据进行剪枝^[45],采用宏森林自动机等方式^[46]实现单层/多层嵌套数据匹配;基于视图的方式为每个用户/角色建立视图,并使用代数式增量、物化视图同步等方式维护视图,用户基于视图进行匹配,提高内存利用率和匹配速度^[47-49]。

现有访问控制策略匹配主要聚焦于对匹配过程的优化,未从策略优化构建的角度来提升匹配效率,需从访问控制策略冗余消除、属性约简等方面展开研究,支撑多源访问控制策略快速匹配。

3.3 策略冲突检测

冲突检测主要包括两类:基于逻辑的冲突检测和基于非逻辑的冲突检测。基于逻辑的方式中,用逻辑系统(如Belnap逻辑、状态修改逻辑)等来表达策略,而后设计基于逻辑的安全策略查询高效评估算法,判断不同策略的相容性。如果相容,则合成,否则基于反例生成等技术溯源冲突点^[50-51]。基于非逻辑的策略冲突检测方面,利用图或树等数据结构表示访问控制策略,并用图/树匹配等方式发现权限分配、传递等过程中的冲突,基于优先级、交互式策略协商等方式自动或半自动消解策略^[52-55]。在策略冲突检测方面,

Berkay 等^[56]提出了一种策略实施系统 IoTGUARD 系统用于识别 IoT 安全策略,针对单个应用或一组交互应用的动态模型实施相关策略并监视策略的实施,能对违规策略及时有效处置。

但现有冲突检测存在效率与可靠性间平衡问题,策略生成技术只适用于简单语义环境,缺乏有效的策略分发与部署机制,未考虑不同节点间协同,需从复杂语义场景下策略自动生成、冲突检测与快速消解、指令有序分发等方面展开研究,支撑跨层级、跨系统、跨域的访问控制策略按需生成。

4 统一授权与延伸控制

授权确保数据使用者拥有为完成任务所必须具备的最小权限,延伸控制是对交换后数据的控制。针对海量多源异构数据的授权和延伸控制的研究主要包括权限分配、权限自动调整和权限延伸控制等方面。

4.1 权限细粒度分配

目前学术界研究重点是云环境下基于属性的权限分配。针对公共云存储环境下单属性授权中心的单点瓶颈和低效率问题,Xue 等^[57]设计了基于多属性授权中心的授权框架,实现了安全高效授权。针对云存储环境下权限动态变更导致的密文频繁更新问题,王晶等^[58]提出了面向云存储的动态授权访问控制机制,从而降低密文更新代价,提高了授权的灵活性。针对授权方不可信或遭受恶意攻击的权限分配问题,关志涛等^[59]提出基于属性加密的多授权中心权限分配方案,提高系统授权效率。针对设备类型多样、用户身份多元等特点,Saxena 等^[60]设计了基于属性的授权方案,大幅降低了通信和计算开销,但方案未考虑授权过程的错误检测与容错性。基于 KP-ABE (key-policy attribute-based encryption),考虑用户关系动态变化,Zhang 等^[61]提出了权限动态分配方案。Bai 等^[62]提出了一种基于多域信息的新角色挖掘框架,利用用户间权限分配关系扩展了角色挖掘技术的能力。现有权限分配主要针对单域信任体系内授权,未考虑多信任体制下权限分配,当前权限分配主要依据单一控制要素,未考虑传播路径等要素对权限分配的影响,需从多信

任体制下多要素融合授权等方面展开研究,支撑跨信任域数据访问权限的自动分配。

4.2 权限自动调整

目前访问权限自动调整主要包括两类:基于风险的权限调整和基于时间的权限调整。在基于风险的权限调整中,首先依据用户场景,定义数据访问所面临的风险指标;而后计算权限调整前和调整所带来的风险,当风险小于预定阈值时,可调整访问权限^[63-66]。基于时间的权限调整方案中,首先设定用户仅在某个时间域内对数据的访问权限,在系统执行过程中,一旦在超出预定时间域,系统自动检测并撤销或调整已分配权限^[67-68]。此外,Yan 等^[69]将上下文感知的信任与声誉评估集成到加密系统,提出了基于信任的访问控制方案,支持访问权限随策略动态变化而调整。综上,现有访问权限的调整主要基于风险和时间等要素,尚未做到权限随访问场景变化而自适应调整。

4.3 权限延伸控制

目前的研究主要聚焦于两方面:基于起源的访问控制(PBAC, provenance-based access control)和 SP (sticky policy) 技术。其中, PBAC 将起源数据作为决策依据,保护起源敏感资源; SP 采用密码学技术将访问控制策略绑定到数据中,确保数据流转。在 PBAC 方面,Sandhu 团队^[70-71]做出了一系列开创性工作,给出了形式化策略规约语言和模型、动态权责分离方案和实施框架。在 SP 技术中,Siani 等^[72]和 Spyra 等^[73]使用加密机制将策略与数据相关联,并对策略进行属性编码和匿名化处理以防止被恶意利用,为全生命周期内数据访问控制提供支持。但这些工作未限定使用哪些要素制定控制决策,未考虑审计信息,不能做到对数据非授权操作的溯源。未来需从延伸策略绑定、共享过程监测、异常共享溯源等方面展开研究,支撑数据全生命周期的可管可控。

5 结束语

随着网络技术、通信技术、安全技术的发展,以及信息利用方式的持续演进,业界期望满足“数据跨域行、按需受控用”的应用需求,确保安全

受控用。本文根据国内外最新研究,对跨域数据流动中的访问控制技术进行了总结和展望,结合复杂应用环境下的访问控制,综述了访问控制模型、数据访问安全模型的发展,分析了访问控制策略管理、统一授权管理、延伸控制等方面的研究现状,总结了存在的问题。

参考文献:

- [1] HONG J N, XUE K P, XUE Y G, et al. TAFC: time and attribute factors combined access control for time-sensitive data in public cloud[J]. IEEE Transactions on Services Computing, 2017.
- [2] XUE Y J, HONG J N, LI W, et al. LABAC: a location-aware attribute-based access control scheme for cloud storage[C]//Proceedings of Global Communications Conference (GLOBECOM). 2016: 1-6.
- [3] DECAT M, LAGASSE B, JOOSEN W. Scalable and secure concurrent evaluation of history-based access control policies[C]//Proceedings of ACM Computer Security Applications Conference (ACSAC), 2015: 281-290.
- [4] YIANNIS V. Context-aware Policy Enforcement for PaaS-enabled Access Control[J]. IEEE Transactions on Cloud Computing, 2019.
- [5] WANG Y C, LI F H, XIONG J B, et al. Achieving lightweight and secure access control in multi-authority cloud[C]//Proceedings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TRUSTCOM). 2015: 459-466.
- [6] ATLAM H F, ALENEZI A, WALTERS R J, et al. Developing an adaptive Risk-based access control model for the internet of things[C]//Proceedings of IEEE International Conference on Internet of Things (iThings). 2017.
- [7] 杨腾飞, 申培松, 田雪, 等. 对象云存储中分类分级数据的访问控制方法[J]. 软件学报, 2017, 28(9): 2334-2353.
YANG T F, SHEN P S, TIAN X, et al. Access control mechanism for classified and graded object storage in cloud computing[J]. Journal of Software, 2017, 28(9): 2334-2353.
- [8] LIU J K, AU M H, HUANG X Y, et al. Fine-grained two-factor access control for web-based cloud computing services[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(3): 484-497.
- [9] ALAM Q, MALIK S U R, AKHUNZADA A, et al. A cross tenant access control (CTAC) model for cloud computing: formal specification and verification[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1259-1268.
- [10] 孙奕, 陈性元, 杜学绘, 等. 一种具有访问控制的云平台下外包数据流动态可验证方法[J]. 计算机学报, 2017, 40(2): 337-350.
SUN Y, CHEN X Y, DU X H, et al. Dynamic authenticated method for outsourcing data stream with access control in cloud[J]. Chinese Journal of Computers, 2017, 40(2): 337-350.
- [11] RONIT N. PolTree: a data structure for making efficient access decisions in ABAC[C]//Proceedings of the 24th ACM Symposium on Access Control Models and Technologies. 2019.
- [12] CHENG Y, PARK J, SANDHU R. An access control model for online social networks using user-to-user relationships[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(4): 424-436.
- [13] SQUICCIARINI A C, LIN D, SUNDARESWARAN S, et al. Privacy policy inference of User-Uploaded images on content sharing sites[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(1): 193-206.
- [14] LI F H, WANG W, MA J F, et al. Action-based access control model[J]. Chinese Journal of Electronics, 2008, 17(3): 396-401.
- [15] 李风华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型[J]. 通信学报, 2016, 37(5): 9-20.
LI F H, WANG Y C, YING L H, et al. Novel cyberspace-oriented access control model[J]. Journal on Communications, 2016, 37(5): 9-20.
- [16] 李风华, 熊金波. 复杂网络环境下访问控制技术[M]. 北京: 人民邮电出版社, 2015.12.
LI F H, XIONG J B. Access control technology for complex network environment[M]. Beijing: POSTS & TELECOM PRESS Co., LTD., 2015.12.
- [17] 李风华, 苏锐, 史国振, 等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.
LI F H, SU M, SHI G Z, et al. Research status and development trends of access control model[J]. Acta Electronica Sinica, 2012, 40(4): 805-813.
- [18] 林果园, 贺珊, 黄皓, 等. 基于行为的云计算访问控制安全模型[J]. 通信学报, 2012, 33(3): 59-66.
LIN G Y, HE S, HUANG H, et al. Behavior-based cloud computing access control security model[J]. Journal on Communications, 2012, 33(3): 59-66.
- [19] 吴泽智, 陈性元, 杨智, 等. 信息流控制研究进展. 软件学报, 2017, 28(1): 135-159.
WU Z Z, CHEN X Y, YANG Z, et al. Survey on information flow control[J]. Journal of Software, 2017, 28(1): 135-159.
- [20] GIACOBBAZZI R, MASTROENI I. Abstract non-interference: a unifying framework for weakening information-flow[J]. ACM Transactions on Privacy and Security, 2018, 21(2): 1-31.
- [21] NIELSON H, NIELSON F. Content dependent information flow control[J]. Journal of Logical and Algebraic Methods in Programming, 2017, 87: 6-32.
- [22] ZHANG J. Cellular clustering-based interference-aware data transmission protocol for underwater acoustic sensor networks[J]. IEEE Transactions on Vehicular Technology (2020).
- [23] 苏锐, 李风华, 史国振. 基于行为的多级访问控制模型[J]. 计算机研究与发展, 2014, 51(7): 1604-1613.
SU M, LI F H, SHI G Z. Action-based multi-level access control model[J]. Journal of Computer Research and Development, 2014, 51(7): 1604-1613.
- [24] LI F H, LI Z F, HAN W L, et al. Cyberspace-oriented access control: model and policies[C]//Proceedings of IEEE International Conference on Data Science in Cyberspace (DSC). 2017: 261-266.
- [25] YU H, JAIN P, KAR P, et al. Large-scale multi-label learning with missing labels[C]//Proceedings of International conference on machine learning (ICML). 2014: 593-601.
- [26] CONG Y, SUN G, LIU J, et al. User attribute discovery with miss-

- ing labels[J]. *Pattern Recognition*, 2018, 73: 33-46.
- [27] GUO K H. LCC: towards efficient label completion and correction for supervised medical image learning in smart diagnosis[J]. *Journal of Network and Computer Applications*, 2019(133): 51-59.
- [28] YIN Y F, SHEN Z J, ZHANG L M, et al. Spatial-temporal tag mining for automatic geospatial video annotation[J]. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 2015, 11(2).
- [29] XU Z Y, STOLLER S D. Mining attribute-based access control policies[J]. *IEEE Transactions on Dependable and Secure Computing*, 2015, 12(5): 533-545.
- [30] YANG Y, YANG Y, SHEN H T. Effective transfer tagging from image to video[C]//*ACM Transactions on Multimedia Computing, Communications and Applications*, 2013, 9(2).
- [31] 王瑜, 武延军, 吴敬征, 等. 基于异构网络面向多标签系统的推荐模型研究[J]. *软件学报*, 2017, 28(10): 2611-2624.
WANG Y, WU Y J, WU Y Z, et al. Multi-dimensional tag recommender model via heterogeneous networks[J]. *Journal of Software*, 2017, 28(10): 2611-2624.
- [32] XIN G. Label distribution learning[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2016, 28(7): 1734-1748.
- [33] LI S W, PURUSHOTHAM S, CHEN C, et al. Measuring and predicting tag importance for image retrieval[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2017, 39(12): 2423-2436.
- [34] WANG G. Hmo: ordering RFID tags with static devices in mobile environments[J]. *IEEE Transactions on Mobile Computing*, 2019(9): 74-89.
- [35] 吴迎红, 黄皓, 曾庆凯. 面向服务访问控制策略精化描述[J]. *计算机研究与发展*, 2014, 51(11): 2470-2482.
WU Y H, HUANG H, ZENG Q K. Description of service oriented access control policy refinement[J]. *Journal of Computer Research and Development*, 2014, 51(11): 2470-2482.
- [36] 林莉, 怀进鹏, 李先贤. 基于属性的访问控制策略合成代数[J]. *软件学报*, 2009, 20(2): 403-414.
LIN L, HUI P J, LI X X. Attribute-based access control policies composition algebra[J]. *Journal of Software*, 2009, 20(2): 403-414.
- [37] MAROUF S, SHEHAB M, SQUICCIARINI A, et al. Adaptive reordering and clustering-based framework for efficient XACML policy evaluation[J]. *IEEE Transactions on Services Computing*, 2011, 4(4): 300-313.
- [38] 牛德华, 马建峰, 马卓, 等. 基于统计分析优化的高性能 XACML 策略评估引擎[J]. *通信学报*, 2014, 35(8): 206-215.
NIU D H, MA J F, MA Z, et al. HP Engine: high performance XACML policy evaluation engine based on statistical analysis[J]. *Journal on Communications*, 2014, 35(8): 206-215.
- [39] 王雅哲, 冯登国, 张立武, 等. 基于多层次优化技术的 XACML 策略评估引擎[J]. *软件学报*, 2011, 22(2): 323-338.
WANG Y Z, FENG D G, ZHANG L W, et al. XACML policy evaluation engine based on multi-level optimization technology[J]. *Journal of Software*, 2011, 22(2): 323-338.
- [40] NGO C, DEMCHENKO Y, LAAT C. Decision diagrams for XACML policy evaluation and management[C]//*Computers & Security*. 2015: 1-16.
- [41] ROSS P, LISCHKAM, MARMOL F G. Graph-based XACML evaluation[C]//*Proceedings of ACM symposium on Access Control Models and Technologies (SACMAT)*. 2012: 83-92.
- [42] LIU A X, CHEN F, HWANG J H, et al. Designing fast and scalable XACML policy evaluation engines[J]. *IEEE Transactions on Computers*, 2011, 60(12): 1802-1817.
- [43] LOU B, LEE D, LEE W C, et al. Qfilter: rewriting insecure XML queries to secure ones using non-deterministic finite automata[J]. *The International Journal on Very Large Data Bases*, 2011, 20(3): 397-415.
- [44] FAN D. Establishment of rule dictionary for efficient XACML policy management[J]. *Knowledge-Based Systems*, 2019(175): 26-35.
- [45] DIAO Y, FISCHER P, FRANKLIN M J, et al. YFilter: efficient and scalable filtering of XML documents[C]//*Proceedings of International Conference on Data Engineering (ICDE)*. 2002: 341-342.
- [46] HAKUTA S, MANETH S, NAKANO K, et al. XQuery streaming by forest transducers[C]//*Proceedings of International Conference on Data Engineering (ICDE)*. 2014: 952-963.
- [47] WU X Y, THEODORATOS D, KEMENTSIETSIDIS A. Configuring bitmap materialized views for optimizing XML queries[J]. *World Wide Web*, 2015, 18(3): 607-632.
- [48] BONIFATI A, GOODFELLOW M, MANOLESCU I, et al. Algebraic incremental maintenance of XML views[J]. *ACM Transactions on Database Systems*, 2013, 38(3): 177-188.
- [49] THIMMA M, LIU F, LIN J Q, et al. HyXAC: hybrid XML access control integrating view-based and query-rewriting approaches[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2015, 27(8): 2190-2202.
- [50] BRUNS G, HUTH M. Access control via Belnap logic: intuitive, expressive, and analyzable policy composition[J]. *ACM Transactions on Information and System Security*, 2011, 14(1): 1-27.
- [51] 吴迎红, 黄皓, 吕庆伟, 等. 基于开放逻辑 R 反驳计算的访问控制策略精化[J]. *软件学报*, 2015, 26(6): 1534-1556.
WU Y H, HUANG H, LYU Q W, et al. Access control policy refinement technology based on open logic r-refutation calculus[J]. *Journal of Software*, 2015, 26(6): 1534-1556.
- [52] HU H X, AHN G, JORGENSEN J. Multiparty access control for online social networks: model and mechanisms[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2013, 25(7): 1614-1627.
- [53] SUCH J M, CRIADO N. Resolving multi-party privacy conflicts in social media[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2016, 28(7): 1851-1863.
- [54] SARKIS L C, SILVA V T D, BRAGA C. Detecting indirect conflicts between access control policies[C]//*Proceedings of Annual ACM Symposium on Applied Computing (SAC)*. 2016: 1570-1572.
- [55] 李瑞轩, 鲁剑锋, 李添翼, 等. 一种访问控制策略非一致性冲突消解方法[J]. *计算机学报*, 2013, 36(6): 1210-1223.
LI R X, LU J F, LI T Y, et al. An approach for resolving inconsistency conflicts in access control policies[J]. *Chinese Journal of Computers*, 2013, 36(6): 1210-1223.
- [56] BERKAY C Z, TAN G, MCDANIEL P D. IoTGuard: dynamic enforcement of security and safety policy in commodity IoT[C]//*NDSS*. 2019.

- [57] XUE K P, XUE Y J, HONG J N, et al. RAAC: robust and auditable access control with multiple attribute authorities for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 953-967.
- [58] 王晶, 黄传河, 王金海. 一种面向云存储的动态授权访问控制机制[J]. 计算机研究与发展, 2016, 53(4): 904-920.
WANG J, HUANG C H, WANG J H. An access control mechanism with dynamic privilege for cloud storage[J]. Journal of Computer Research and Development, 2016, 53(4): 904-920.
- [59] 关志涛, 杨亭亭, 徐茹枝, 等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报, 2015, 36(6): 116-126.
GUAN Z T, YANG T T, XU R Z, et al. Multi-authority attribute-based encryption access control model for cloud storage[J]. Journal on Communications, 2015, 36(6): 116-126.
- [60] SAXENA N, CHOI B J, LU R. Authentication and authorization scheme for various user roles and devices in smart grid[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 907-921.
- [61] ZHANG Y, CHEN J, DU R Y, et al. FEACS: a flexible and efficient access control scheme for cloud computing[C]//Proceedings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TRUSTCOM). 2015: 310-319.
- [62] BAI W. RMMDI: a novel framework for role mining based on the multi-domain information[C]//Security and Communication Networks 2019.
- [63] KHAMBHAMMETTU H, BOULARES S, ADI K, et al. A framework for risk assessment in access control systems[J]. Computers & Security, 2013, 39: 86-103.
- [64] MIETTINEN M, HEUSER S, KRONZ W, et al. ConXsense: automated context classification for context-aware access control[C]//Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIA CCS). 2014: 293-304.
- [65] SANTOS D, RICARDO D, WESTPHALL C M, et al. A dynamic risk-based access control architecture for cloud computing[C]//Proceedings of Asia-Pacific Network Operations and Management Symposium (NOMS). 2014: 1-9.
- [66] 惠榛, 李昊, 张敏, 等. 面向医疗大数据的风险自适应的访问控制模型[J]. 通信学报, 2015, 36(12): 190-199.
HUI Z, LI H, ZHANG M, et al. Risk-adaptive access control model for big data in healthcare[J]. Journal on Communications, 2015, 36(12): 190-199.
- [67] NING J T, CAO Z F, DONG X L, et al. Auditable -time outsourced attribute-based encryption for access control in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 94-105.
- [68] YANG K, LIU Z, JIA X H, et al. Time-domain attribute-based access control for cloud-based video content sharing: a cryptographic approach[J]. IEEE Transactions on Multimedia, 2016, 18(5): 940-950.
- [69] YAN Z, LI X Y, WANG M J. Flexible data access control based on trust and reputation in cloud computing[J]. IEEE Transactions on Cloud Computing, 2017, 5(3): 485-498.
- [70] NGUYEN D, PARK J, SANDHU R. A provenance-based access control model for dynamic separation of duties[C]//Proceedings of International Conference on Privacy, Security and Trust (PST). 2013: 247-256.
- [71] SUN L, PARK J, NGUYEN D, et al. A provenance-aware access control framework with typed provenance[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(4): 411-423.
- [72] SIANI P, CASASSA-MONT M. Sticky policies: an approach for managing privacy across multiple parties[C]//Computer, 2011, 44(9): 60-68.
- [73] SPYRA G, BUCHANAN W J, EKONOMOU E. Sticky policies approach within cloud computing[J]. Computers & Security, 2017, 70: 366-375.

[作者简介]



诸天逸(1995-), 男, 江苏无锡人, 中国科学院信息工程研究所博士生, 主要研究方向为跨域访问控制。



李凤华(1966-), 男, 湖北浠水人, 博士, 中国科学院信息工程研究所研究员、博士生导师, 主要研究方向为网络与系统安全、大数据安全与隐私保护、密码工程。



成林(1983-), 男, 河北邢台人, 博士, 中国信息安全测评中心助理研究员, 主要研究方向为云计算安全、大数据安全。



郭云川(1977-), 男, 四川营山人, 中国科学院信息工程研究所正研级高级工程师、博士生导师, 主要研究方向为访问控制、形式化方法。