基于属性的访问控制关键技术研究综述

房 梁[1),2),3)] 殷丽华[2),3)] 郭云川[2),3)] 方滨兴[1),2)]

[1)](北京邮电大学计算机学院 北京 100876)

[2)](中国科学院信息工程研究所信息内容安全国家工程实验室 北京 100093)

[3)](中国科学院信息工程研究所物联网信息安全技术北京市重点实验室 北京 100093)

摘 要 云计算、物联网等新型计算模式为我们提供了便捷的数据共享、高效计算等服务,极大地提高了数据的处理效率,提升了计算和存储资源的利用能力.但这些新型计算模式存储并融合了大量具有"所有权"特征的数据,如果不对这些数据提供可靠的保护,一旦泄漏就会给用户带来巨大的损失.作为数据保护的基石性技术之一,访问控制可保障数据仅能被拥有相应权限的用户访问,得到了广泛的研究.其中,基于属性的访问控制通过使用属性作为访问控制的关键要素,有效解决了具有大规模、强动态性及强隐私性特点的新型计算环境下的细粒度访问控制问题,为云计算、物联网计算等新型计算环境提供了理想的访问控制策略.该文将基于属性的访问控制的整体流程分为准备阶段和执行阶段,并对两阶段面临的关键问题、研究现状和发展趋势进行分析.针对其中的实体属性发现、权限分配关联关系挖掘、访问控制策略描述、多机构合作、身份认证、权限更新与撤销等难点问题进行深入探讨.最后,在对已有技术进行深入分析对比的基础上,指出未来基于属性的访问控制的研究方向.

关键词 基于属性的访问控制;实体属性发现;权限分配关联关系;策略描述;多机构合作;身份认证;权限更新与撤销

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01680

A Survey of Key Technologies in Attribute-Based Access Control Scheme

FANG Liang[1),2),3)] YIN Li-Hua[2),3)] GUO Yun-Chuan[2),3)] FANG Bin-Xing[1),2)]

[1)](*School of Computer Science, Beijing University of Posts and Telecommunications, Beijing* 100876)

[2)](*National Engineering Laboratory for Information Security Technologies, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[3)](*Beijing Key Laboratory of IOT Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

Abstract New computing paradigms, including Cloud Computing and Internet of Things(IOTs) provide us convenient services such as data sharing and effective computing. It greatly improves the efficiency of data processing and makes full use of the computing and storage resources. However, huge number of data with specific ownership also stored in these new computing paradigms. If they don't obtain efficient protection, it will bring serious risks of data leakage, thus causing tremendous loses for users. Therefore, measures should be taken to make sure that the data only can be accessed by users with appropriate permissions. Access control, which can be used to prevent unauthorized access, attracts extensive attention from both academia and industry. Among the access control schemes, Attribute-Based Access Control(ABAC), which takes attributes as the key element to build up the whole access control system, is the most suitable scheme to achieve fine-grained access control for the new computing paradigms which have features such as large

收稿日期:2015-11-12;在线出版日期:2016-04-10.本课题得到国家重点研究发展计划基金资助项目(2016YFB0800303)、中国科学院战略性先导科技专项(XDA06030200)资助.**房 梁**,男,1989 年生,博士研究生,主要研究方向为物联网安全、访问控制等. E-mail:fangliang_iie@163.com. **殷丽华**(通信作者),女,1973 年生,博士,副研究员,主要研究方向为网络安全、安全性评估等. E-mail:yinlh_iie@163.com. **郭云川**,男,1977 年生,博士,副研究员,主要研究方向为安全性评估、形式化方法和物联网安全. **方滨兴**,男,1960 年生,博士,教授,博士生导师,中国工程院院士,主要研究领域为网络安全和信息内容安全.

scale, dynamicity and strong privacy need etc. With the help of ABAC, we can provide an ideal access control system for computing paradigms like Cloud Computing and Internet of Things. In this paper, we discuss and analyze the existing problem, current research situation and development trend in the preparation and executing stage of ABAC. In particular, we elaborate the researches including the entity attributes mining, permission allocate mining, access control policy specification, multi-authorities research, user identity and access permission management. Finally, possible future work and some conclusions are pointed out.

Keywords　attribute-based access control; attributes mining; permission allocate mining; policy specification; multi-authorities; user identity; permission management

1　引　言

云计算、物联网等新型计算环境为我们提供了便捷的数据共享、融合计算等服务，极大地提高了对数据的处理效率，使计算和存储资源得到充分的利用. 其中包含了大量的具有“所有权”特征的个人隐私数据，然而，对这些信息的保护却不尽如人意. 这些隐私信息与个人隐私或机构利益密切相关，一旦泄漏则可能会带来巨大的损失. 从韩国三大信用卡公司信息泄露事件①，到 iCloud 云端系统漏洞风波②，这些隐私数据泄漏事件使得用户对通过新型计算环境获取数据服务时的数据安全性提出了质疑. 隐私数据必须要满足“有限公开”原则，即只有授权用户才能搜索到授权允许访问的信息.

访问控制技术根据预先设定的访问控制策略，保障资源只能被合法用户执行合法操作，防止了信息的非授权访问. 访问控制的研究及发展大致可分为以下 4 个阶段：第 1 阶段(20 世纪 70 年代)是应用于大型主机系统中的访问控制，代表性工作是分别保障机密性和完整性的 BLP 和 Biba 模型. 第 2 阶段(20 世纪 80 年代)，随着对计算机的可信要求度提高，研究者提出了更为灵活的访问控制方案，标志工作是美国国防部提出的可信计算机系统评估准则(TCSEC). 根据该标准，依据访问权限管理者角色的不同，访问控制可分为自主访问控制(Discretionary Access Control，DAC)和强制访问控制(Mandatory Access Control，MAC). 第 3 阶段(2000 年左右)，随着信息系统在企事业单位的大规模应用和互联网的日趋繁荣，DAC 和 MAC 的有限扩展等本质特征使得其难以处理日益复杂的应用层访问需求. 作为一种有效的解决手段，基于角色的访问控制(Role-Based Access Control，RBAC)应运而生. 本质上，“角色”匹配于企事业单位的组织结构. 第 4 阶段，随着云计算、物联网等新型计算环境的出现，新型计算环境所具有的一些特点给访问控制技术的应用带来了巨大的挑战，使得传统的面向封闭环境的访问控制模型如 DAC，MAC，RBAC 等难以直接适用于新型计算环境. 具体来说：(1) 海量性. 在封闭环境中，用户和资源的数量有限. 但在新型计算环境下，终端数量和用户数量庞大，根据 2013 年 5 月工业和信息化部发布的《物联网标识白皮书》，未来我国的物联网终端数量将达到 100 亿～1000 亿. 传统的访问控制系统采用静态的访问控制管理方式对用户及其相应的权限进行管理，这种方式需要存储大量的用户及权限信息. 但由于用户及资源的海量特性，维护和存储一个庞大的访问控制列表会带来极大的存储和管理负担，同时在对用户权限查询时效率非常低；(2) 动态性. 新型计算环境下，节点和用户在不断移动，访问数据对象实时变化；同时，节点可能不断接入和退出，体现出很强的动态性. 传统的访问控制机制要求预先设定用户-权限的对应关系，但这种动态性使得我们无法提前预知所有用户信息，也无法准确了解用户和权限结构，更无法提前预设用户-权限对应关系. 此外这种动态性使得访问控制对于访问控制策略更新的实时性更加敏感，同时传统访问控制机制采用单一的授权机构的管理方式，海量用户的频繁变化，会带来非常大的管理及运算负担；(3) 强隐私性. 随着公共平台上信息的共享程度越来越高，对数据隐私和个人隐私信息的保护提出了更高的要求. 大多数服务提供商通过明文方式进行数据存储，一旦存储服务器被黑客攻破，用户存储的所有数据将会被泄露，例如 2014 年 2 月，eBay 近 1.28 亿用户的个人信息遭到黑客恶意泄

① http://korea.people.com.cn/205155/205166/8518347.html

② http://www.bbc.co.uk/newsbeat/article/29008876/jennifer-lawrence-nude-photos-leaked-after-icloud-hack

露①.为了使用户可以放心地将自己的数据交付于数据服务提供商,除需要对用户的访问操作进行控制外,还需考虑对数据本身的保护.

基于用户、资源、操作和运行上下文属性所提出的基于属性的访问控制(Attribute-Based Access Control,ABAC)将主体和客体的属性作为基本的决策要素,灵活利用请求者所具有的属性集合决定是否赋予其访问权限,能够很好地将策略管理和权限判定相分离.由于属性是主体和客体内在固有的,不需要手工分配,同时访问控制是多对多的方式,使得 ABAC 管理上相对简单.并且属性可以多个角度对实体进行描述,因此可根据实际情况改变策略.例如针对时间约束所提出的基于时态特性的访问控制模型通过分析用户在不同的时间可能有不同的身份,将时态约束引入访问控制系统中,通过时间属性来约束用户的访问操作[1];又比如基于使用的访问控制模型(Usage Control,UCON)引入了执行访问控制所必须满足的约束条件(如系统负载、访问时间限制等)[2].除此之外,ABAC 的强扩展性使其可以同加密机制等数据隐私保护机制相结合,在实现细粒度访问控制的基础上,保证用户数据不会被分析及泄漏.例如,基于属性的加密(Attribute-based Encryption,ABE)方法[3].

上述优点使 ABAC 能够有效地解决动态大规模环境下的细粒度访问控制问题,是新型计算环境中的理想访问控制模型,应用前景广阔.本文针对 ABAC 中准备阶段和执行阶段所需解决的关键问题,详细分析了 ABAC 中的关键技术,对 ABAC 的理论研究进行了分析和总结.最后,我们对 ABAC 面临的挑战及今后的研究趋势进行讨论,以期为新型计算环境下的访问控制研究提供思路和参考.

2 基于属性的访问控制模型

2.1 ABAC 基本模型

属性是 ABAC 的核心概念,ABAC 中的属性可以通过一个四元组(S,O,P,E)进行描述[4].S 表示主体(Subject)属性,即主动发起访问请求的所有实体具有的属性,如年龄、姓名、职业等;O 表示客体(Object)属性,即系统中可被访问的资源具有的属性,如文档、图片、音频或视频等数据资源;P 表示权限(Permission)属性,即对客体资源的各类操作,如文件或数据库等的读、写、新建、删除等操作;E 表示环境(Environment)属性,即访问控制过程发生时的环境信息,如用户发起访问时的时间、系统所处的地理或网络位置、是否有对同一信息的并发访问等信息,这一属性独立于访问主体和被访问资源.

如图 1 所示,ABAC 系统按其执行操作种类的不同可分为两个阶段:准备阶段和执行阶段.准备阶段主要负责收集构建访问控制系统所需的属性集合以及对访问控制策略进行描述.而执行阶段主要负责对访问请求的响应及对访问策略的更新.首先,属性权威(Attribute Authority,AA)预先收集,存储和管理构建安全的访问控制所需的所有属性以及属性-权限之间的对应关系.因此为了构建安全的 ABAC,首先需要从海量的类型各异的访问主体和访问客体挖掘出独立、完备的主体属性、客体属性、权限属性和环境属性集合,并构建这些属性同相关实体之间的关联关系.属性的独立性保证了属性集合中不存在意义相似的冗余属性,减小了系统的存储和管理负担.完备性则保证了属性集合可以提供访问控制系统所需的所有属性,保证了系统的安全性.因此独立完备的实体属性发现技术是 ABAC 研究中的基础.当获得属性集合后,需要对属性与权限之间的对应关系进行分析.传统的访问控制机制大多通过专家分析企业的业务流程,抽象并完成属性-权限的分配关系,但是由于依赖专家对环境的了解,人工依赖性较强.面对开放性极强的新型计算环境,几乎没有专家能对整个应用场景有完整的了解,导致自顶向下的方法并不适用.因此自动化的属性-权限关联关系发现方法是需要解决的重要问题.当获取独立完备的属性集合以及属性-权限对应关系后,策略管理点(Policy Administration Point,PAP)利用这些信息对访问控制策略进行形式化描述.不同的访问控制策略描述方法有不同的表达能力,但目前的方案中,表达能力的提升伴随着访问控制策略复杂度的提高.因此设计复杂度较低且具有丰富表达能力的访问控制描述语言可以保证 ABAC 系统高效准确运行.此外,随着新型计算环境的发展,不同域间的资源共享和信息互访日益增多.但不同的域系统往往是独立的,每个不同的域具有自己独特的访问控制策略,一个域中的用户拥有的权限往往在另一个域内会失效.因此在保证自身访问控制安全的基础上,实现多域间不同策略的翻译、融合可以最大限度地保障不同自治域间安全的资源共享和信息交互.

① http://wallstreetpit.com/104110-ebay-ebay-hacked/

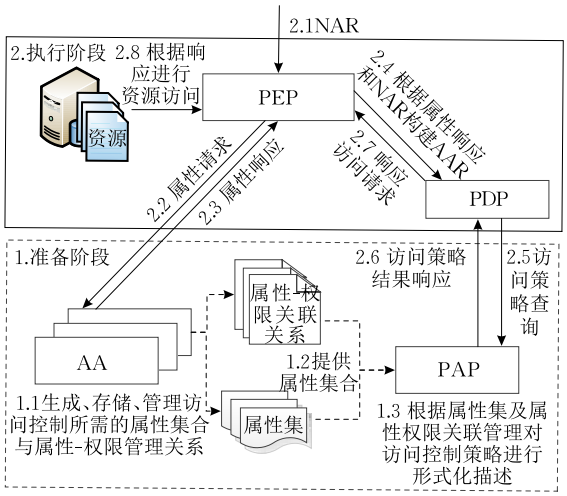


图 1　ABAC 机制框架示意图

在执行阶段中，当接收到原始访问请求(NAR)之后，策略实施点(Policy Enforcement Point，PEP)向 AA 请求主体属性、客体属性以及相关的环境属性，并根据所返回的属性结果集构建基于属性的访问请求(AAR)并将 AAR 传递给策略决策点(Policy Decision Point，PDP). PDP 根据 AA 所提供的主体属性、客体属性以及相关的环境属性，对用户的身份信息进行判定. 通过与 PAP 进行交互，根据 PAP 提供的策略查询结果对 PEP 转发来的访问请求进行判定，决定是否对访问请求授权，并将判定结果传给 PEP. 最终由 PEP 执行判定结果. 但是在 ABAC 中用户的身份是由一系列属性组成的集合来表示，具有较强的匿名性，这种匿名性导致用户可能滥用其所拥有的属性带来的权限. 通过引入身份认证机制可以有效保证用户所提供属性的可靠性及数据源的不可否认性，增强访问控制系统的安全性. 同时新型计算环境中用户和设备的动态特性带来了权限的频繁变动，需要对这些变动实时响应，更改相应的权限，保证系统安全可靠的运行.

综上，实体属性发现机制、属性-权限关联关系发现机制、访问控制策略描述机制、访问控制中的多域合作机制、身份认证机制，权限实时更新机制是目前 ABAC 中较为重要的研究点.

2.2　ABE 基本概念

虽然传统的 ABAC 有效控制了用户对资源的访问操作，但其仅实现了对用户访问过程的控制. 而随着云和物联网等新型计算环境产生并存储的敏感隐私信息日益增多，由信息泄露所导致的安全威胁也不断增加. 因此，为了最大限度的保护数据的隐私安全，实现更细粒度的访问控制，研究者们提出了基于属性的加密机制(Attribute-Based Encryption，ABE)[3]. ABE 实现了对数据机密性的访问控制. 其采用非对称密码机制并利用属性作为加解密的关键要素，将属性同密文和用户密钥相结合. 当用户属性与密文属性的公共集合满足加密时访问结构所规定的参数时才能解密相应数据.

如图 2 所示 ABE 机制也可分为准备阶段和执行阶段. 准备阶段中 AA 的任务同传统 ABAC 中相同，负责预先收集，存储和管理构建安全的访问控制所需的所有属性. Authority 根据不同的访问结构及属性设计访问控制策略，并将这些策略封装在资源加密密钥或用户解密密钥中. 依据访问控制策略制定者角色的不同，ABE 可以细化为以下两类：基于密钥策略的 ABE(Key-Policy Attribute-Based Encryption，KP-ABE)[5] 和基于密文策略的 ABE(Ciphertext-Policy Attribute-Based Encryption，CP-ABE)[6]. KP-ABE 方案中，用以描述访问控制策略的访问结构同用户私钥相结合，属性集合同待访问资源相关联. 这种方式下访问控制策略由数据接收方设定，用户可以设定接收特定的消息，用户自由度较高. 而数据拥有者由于仅能使用属性对数据进行描述，无法设定相应的访问控制策略，因此对其数据的控制较弱. KP-ABE 比较适合付费电视、视频点播等系统[7]. 而 CP-ABE 方案则与 KP-ABE 相反，此时用以描述访问控制策略的访问结构同待访问资源相结合，属性集合同用户私钥相关联. 这种方式下访问控制策略由数据拥有者设定，数据拥有者自由度较高. CP-ABE 机制比较适用于访问控制类业务，如电子医疗健康记录访问[8]、社交网站访问[9]等系统.

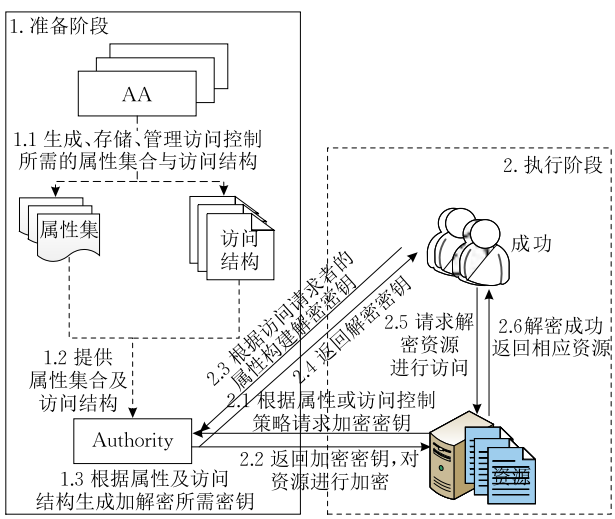


图 2　ABE 机制框架示意图

在执行阶段中,用户通过 AA 获取相关的属性并根据自身属性向 Authority 请求解密私钥,之后利用所获取的密钥对密文进行解密并返回最终结果.表 1 列出了 KP-ABE 和 CP-ABE 机制执行阶段的输入和输出的对比.

同传统的 ABAC 机制各阶段所面临的问题相同,ABE 机制也面临着实体属性发现、属性-权限关联关系发现、访问控制策略描述、多域合作、身份认证、权限更新等问题.而新型计算环境下大量用户和各类设备具有的属性的频繁变化带来了与该用户属性相关的所有用户的密钥和相应密文的频繁更新,而密文和密钥的计算需要耗费大量的计算资源,因此 ABE 机制中的权限更新问题尤为突出.如何平衡更新粒度及计算资源消耗的权限更新机制是 ABE 中的重要问题.

表 1 KP-ABE 和 CP-ABE 对比

		KP-ABE	CP-ABE
Setup(λ,U)	输入	安全参数 属性空间大小 用户空间大小	安全参数 属性空间大小 用户空间大小
	输出	公钥参数 PK	公钥参数 PK
Encrypt(PK,M,A)	输入	主密钥 MK 公钥参数 PK 信息 M 属性集合 γ	主密钥 MK 公钥参数 PK 信息 M 访问结构 A
	输出	加密数据 CT	加密数据 CT
KeyGen(MK,S)	输入	主密钥 MK 访问结构 A 公钥参数 PK	主密钥 MK 属性集合 γ NA
	输出	解密密钥 D	用户私钥 SK
Decrypt(PK,CT,SK)	输入	公钥参数 PK 加密数据 CT 解密密钥 D	公钥参数 PK 加密数据 CT 用户私钥 SK
	输出	原始数据 M	原始数据 M

因此,本文第 3～8 节分别对目前 ABAC 中有关实体属性发现机制、属性-权限关联关系发现机制、访问控制策略描述机制、访问控制中的多域合作机制、身份认证机制、权限实时更新机制的研究进行详细的分析与总结,最后在第 9 节阐述了今后研究所面临的挑战和发展方向.

3 实体属性发现机制研究

访问对象和被访问对象存在大量的固有属性,属性选取的好坏直接影响访问控制系统的性能.在引入链接服务(Linking Service,LS)的基础上首次提出了属性聚合的概念模型[10-11],并针对联邦身份管理提出了可信属性聚合框架.链接服务指将多个用户身份提供商(Identity Providers,IdP)相关联的可信第 3 方.LS 通过融合多个 IdP 所包含的用户属性信息,并根据每个 LS 提供信息的可靠程度生成一个完整的用户属性.然而该方案中 IdP 提供信息的可信程度相对固定,未考虑 IdP 在工作过程中信誉的变化.为此,通过引入节点信任度的概念研究者提出了一种基于多节点合作的属性聚合方法[12].当出现系统无法识别的属性时,该方法从多个相互合作的节点获取属性.参与合作的节点之间根据背景知识相互计算与之相连的邻居节点的信誉值,并在服务提供商(Service Providers,SP)进行属性查询时将信誉值上传.SP 对所有的信誉值进行计算后根据事先设定好的阈值判断提供属性信息的节点是否可信,对不可信的节点所提供的信息进行过滤,保证结果的准确性.该方法较好地解决了属性聚合中的信誉问题.此外,为了解决多属性的聚合操作问题,文献[13]在权重聚合、诱导聚合的基础上提出多向量汇聚操作符 AgOp,在功能上聚合了属性.但该方案并未考虑属性聚合所带来的安全问题.例如传统的属性聚合方法需要一个固定的共享唯一标识,一旦共享标识泄漏则会造成用户信息的泄漏.针对这一问题,文献[14]基于 SAML 提出了一种不需要利用固定的唯一共享标识进行属性聚合的方法.通过 OpenID 防止攻击者关联用户行为,实现隐私聚合.又比如 ABAC 系统中属性的获取通常是通过预先设定好的属性权威,当服务请求者包含属性权威无法识别的属性时,ABAC 系统就无法提供正常的服务.此外,为了兼顾数据可用性和隐私安全性,需要在保证聚类结果可用性的基础上对敏感信息进行隐藏.因此文献[15]提出了基于保邻域隐藏的扰动算法.通过分析数据点的邻域结构,给出了能够保持数据邻域组成稳定的安全邻域定义并提出等价置换弧的概念.通过随机选取与待隐藏策略位于相同安全邻域内的等价置换弧上的点并与之进行替换的方法对隐私信息进行隐藏.但该方法对所有样本和属性采取相同的隐私保护强度,但在实际应用中不同的样本和属性有着不同的敏感等级,因此需要采取不同粒度的保护方法.针对这种需求,研究者提出了一种改进的基于奇异值分解数据扰动的隐私保持分类挖掘方法[16].

为了定量地描述属性和实体之间的关联关系,文献[17]提出了一种基于概率模型的学习方式,利用事先设定好的抽取规则和已有的字典首先抽取出不同的实体、概念和属性,并统计给定概念时某一属

性的出现次数和给定属性时某一概念的出现次数，之后利用贝叶斯概率模型对属性进行打分将属性值和对应的概念相关联，从而实现最优属性的挖掘.此外，针对最优属性的研究还包括：采用无监督学习等方式对属性同义词进行挖掘[18]，基于垂直搜索网站超链接语义的潜属性信息发现技术[19]，根据待抽取属性自身结构和内容的特点，通过定义一系列规则和证据所提出的基于可信度分析发现 Web 页面新属性的方法[20]等.

虽然目前属性发现的研究已经取得了一定的研究成果，但针对噪音环境下大规模数据的独立、完备的属性挖掘方法仍较为欠缺.独立完备的属性集合是构建 ABAC 的基础.属性的独立保证构建访问控制所需的属性集中不包含意义重复的冗余属性.而属性的完备则保证了属性集满足准确地响应访问请求所需的所有属性.因此在满足独立完备的约束的条件下，如何设计出优良的算法以较低的计算复杂度来得到尽可能好的查询属性集是今后需要解决的关键科学问题.

4　属性-权限关联关系发现方法研究

新型计算环境中多样的用户和设备带来了海量的不同属性.这些属性包含大量构建访问控制系统所不必需的冗余属性，我们不可能对其进行手工筛选.因此，需对自动化的用户-属性、属性-权限关联关系方法进行研究.但目前针对用户-属性、属性-权限之间关系的研究仍较为欠缺，而 RBAC 可看作是 ABAC 的单属性特例，通过借鉴 RBAC 中的角色工程方法可以为属性工程的研究提供思路.角色工程可分为自顶向下和自底向上两大类.

4.1　自顶向下方法

自顶向下方法指借助于专家所具备的相关知识，通过专家对企业的安全需求和业务流程进行分析，抽象出角色集，并完成角色-权限的分配关系，最终达到构建安全的访问控制系统的目的[21].在此基础上，研究者们提出了不同的解决方案.文献[22]通过定义使用用例(use case)的方法提出了一种自顶向下的构建方法.通过找出企业所有的使用用例序列，分析出满足企业安全需求的所有权限和相应的角色，并通过这些角色对使用用例进行映射从而构建安全的访问控制.此外，通过利用场景分析法也可以生成在不同场景下访问所需的不同权限，进而得到合适角色[23].该方法通过逐层分解的方法逐步将企业安全需求细化，将工作分解成任务、任务分解成场景、场景分解成步骤、步骤分解成权限，最后根据所得到的权限构建 RBAC 系统.

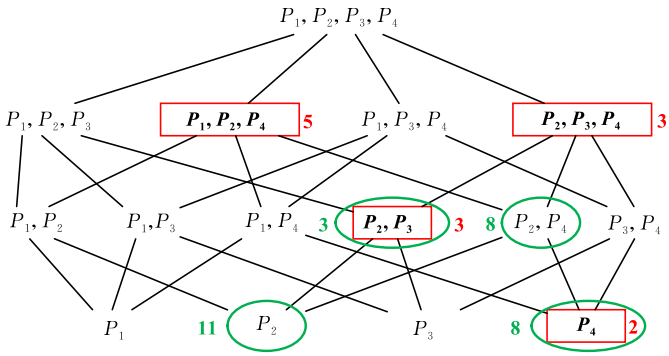
自顶向下的方法可以构建出满足真实应用场景的用户-角色及角色-权限关联关系，但这类方法主要依赖专家对真实应用场景的了解，人工依赖性较强.当面对云和物联网等新型计算环境时，几乎没有专家能对全部的应用场景有完整的了解，导致这种方法难以直接应用.

4.2　自底向上方法

针对自顶向下方法人工依赖性较强的问题，研究者提出了自底向上的方法，自底向上的方法在已有“用户-权限”对应关系的基础上，利用数据挖掘技术或矩阵分解的方法自动筛选生成候选角色集合，使得获得的“用户-角色”与“角色-权限”的笛卡尔积尽量逼近原“用户-权限”关系.依据候选角色集合算法输出结果的不同，自底向上的方法可划分为两类：基于候选角色输出的算法和基于角色状态输出的算法.第 1 类方法生成一定的候选集合并按照一定的阈值确定最终候选角色，第 2 类方法除生成角色集合外，还生成完整的角色状态，包括：用户和角色之间的分配关系、角色和权限之间的分配关系、角色之间的层次关系.

针对第 1 类算法，研究者们提出了不同的解决方案.例如利用聚类算法的角色挖掘方法通过对用户进行分类，每一类用户集对应一个角色，然后利用关联规则挖掘角色所对应的权限[24].但是该方案并未对生成的角色集合进行排序，缺乏对所生成角色优劣的度量方法，增加了管理员选取候选角色的难度.针对该问题，基于枚举及排序的思想，研究者提出一种称之为 Complete Miner 的候选角色生成排序算法，该算法通过枚举用户权限之间的交集，之后对生成的新集合求交集，直到枚举出了所有可能的集合.最后对所枚举出的集合按照其包含用户的数量进行排序[25].如图 3 所示，方框中的集合代表原始数据中生成的权限集合，椭圆形框中集合代表求交集后新生成的权限集合.这种方式的时间复杂度随着求交前角色数量呈指数级增长.为此，作者将枚举过程限制为仅枚举两两初始化角色之间的交集，以此降低时间复杂度，提出了 Fast Miner 的方法.除此之外，相关的挖掘方法还包括利用关联规则挖掘进行角色挖掘[26]，采用 PF-tree 算法找到权限集簇的一个子集作为角色集从而对权限集合进行挖掘[27]等.这类方法虽然实现较为简单，可以利用已

User	P_1	P_2	P_3	P_4
u_1	0	0	0	0
u_2	1	1	0	1
u_3	0	1	1	0
u_4	1	1	0	1
u_5	1	1	0	1
u_6	0	1	1	1
u_7	0	1	I	1
u_8	0	1	1	0
u_9	0	I	1	0
u_{10}	0	0	0	1
u_{11}	0	0	0	1
u_{12}	0	0	0	0
u_{13}	1	1	0	1
u_{14}	1	1	0	1
u_{15}	0	1	1	1



	Original Count	Generated Count
P_1, P_2, P_4	5	0
P_2, P_3, P_4	3	0
P_2, P_3	3	3
P_2, P_4	0	8
P_2	0	11
P_4	2	8

图 3 Complete Miner 方法[25]

有的一些聚类方法生成角色候选集合，并根据不同的情景利用不同的先验知识选取对应的阈值，从而达到从候选集合中选取角色集合的目的. 但缺乏对所生成角色优劣的有效度量方法，同时现有的度量方法大多需要人为的选取设置一个合理的阈值，使得结果仍具有一定的主观性，与专家对系统的了解程度有关. 此外，这类方法并未考虑所生成的角色集合所包含的用户-权限对应关系与原始的用户-权限对应关系的差异，所生成的角色集合与原始数据可能存在较大偏差.

第 2 类方法的提出一定程度上解决了第 1 类方法的缺点. 研究者给出了通过寻找可最大程度覆盖权限的角色集生成最终角色的方法[28-32]. 其中文献[30]在将矩阵分解的概念引入了角色挖掘的基础上，根据新生成的用户-权限对应关系与原始的用户-权限对应关系之间的覆盖率给出了角色挖掘问题中不同变种的定义. 基本角色挖掘问题定义要求所生成的新用户-权限对应关系可以完全匹配原始的权限分配关系. 但是由于定义中要求所生成的新用户-权限对应关系与原始关系完全一致，当系统中的权限分配比较分散时，为了满足约束条件，所生成的角色数有可能会很大. 假设有以下场景：访问控制系统中有 1000 个用户和 100 个权限，5000 个用户-权限对应关系. 假设我们实现完全完整准确的矩阵分解生成 100 个角色. 但是如果只需要 50 个角色就可以匹配 99%的用户-权限分配关系(4950 个用户-权限分配关系)，那么相比于由于角色增加所带来的系统管理负担的增加，少量的原始数据的损失是可以接受的. 因此允许挖掘出的角色具有一定的冗余性具有很强的现实意义. 为了解决这一问题，研究者给出了 δ-近似角色挖掘的定义和解决方案[30]. 该方案允许挖掘出的权限分配关系与原始关系相比有一定的差异. 此外，有些访问控制系统需要严格控制角色的数量，只需要在满足角色数量的前提下尽可能地覆盖所有的 UPA 即可，针对这种情况给出了最小噪音挖掘问题的定义. 作者针对以上所给出的定义，通过将角色挖掘映射到 Minimum Tiling 问题和 Discrete Basis 问题上，给出了相应的解决方案，同时证明了角色挖掘方法是一个 NPC 难题. 另外，基于分块思想，文献[31]提出了一种从角色-权限矩阵找出能覆盖所有权限的最小角色集合的方法. 而通过利用概率模型也可将 RBAC 中的角色挖掘问题转换为一种概率统计问题，并对生成的角色进行优化[32]. 除此之外，采用图论知识将角色挖掘问题转换为图的优化问题可以有效改进第 1 类方法缺乏层次、候选角色较多和精确度较低等缺陷. 在文献[28]的基础上，研究者基于最小二部图覆盖理论提出了一个启发式算法 HP Role Minimization，该方法解决角色挖掘问题，使求得的角色数最优[29]. 虽然该方法得到的角色数最小，但是单纯追求角色数最少并不一定最好，追求角色数最少通常是以牺牲精确度为代价的.

此外，通过研究新挖掘出的属性具有的语义关系和度量新挖掘出的属性集合同原始访问控制系统中属性集合之间的相似度，可以有效地保证依据新挖掘出的属性集构建的访问控制系统同原始访问控

制系统语义上保持一致性.针对语义问题,文献[33]通过引入概念格(Concept Lattices)的方式,利用概念格自身的层次特性,构建用户和权限之间的分配层次关系,并通过对概念格的分析生成相应的角色.这种方法保证了挖掘出的角色具有更好的语义信息.而概率模型的引入使得用户权限之间分配关系以及描述商业信息的角色可以通过不同商业信息间的相关联性分析进行反映[34].针对同原始数据的相似度度量问题,研究者提出了利用 Jaccard Coefficient[35],Hamming Distance[32]等方法的角色集之间的相似度度量方法.但这些方法仍缺乏多属性之间语义关联度的研究.同时,原始数据中的噪音数据很大程度上影响了挖掘结果的准确性,如何处理原始数据中的噪音问题是今后值得关注的研究点.

5　ABAC 中访问控制策略描述研究

对不同用户和资源的安全需求进行准确有效的形式化描述可以保证访问控制系统对各类访问请求做出准确的响应.因此设计表达能力丰富的访问控制策略描述方法是 ABAC 研究中的重要问题.

针对传统的 ABAC 的策略描述问题,研究者们提出了分层 CLP 中的集合描述法[36]、安全断言标记语言(Security Assertion Markup Language,SAML)[37]、可扩展访问控制标记语言(Extensible Access Control Markup Language,XACML)[38]等描述方法.其中,XACML 定义了策略的标准表示格式以及做出授权决策的标准方法.这些标准使根据 XACML 制定的访问控制策略具有通用性,可以在多个不同的系统中使用相同的 XACML 描述策略,比较适用于分布式环境下的访问控制策略描述.此外,XACML 继承了 XML 的平台无关性特点,可以有效地嵌套进现有的系统中而无需对现有系统结构进行改变.XACML 的这些特点使其已被广泛应用于 ABAC 的研究中.目前在实际应用环境中比较常见的 XACML 标准包括 XACML3.0①、SunXACML②、NDG_XACML③ 等.针对 XACML 在实际应用中面临的挑战,研究者们提出了不同的解决方案.针对网格系统中大量易变的数据,通过扩展 XACML 对其数据进行封装重新描述,研究者提出了一个支持网格计算的授权框架[39].为了保障云计算中的安全,通过对原始 XACML 进行扩展提出了分布式细粒度的授权方法[40].文献[41]则基于 XACML 为云计算中的外包数据提出了层次化的 ABAC 控制框架,增加了访问控制策略描述方法的灵活性,可以有效地在策略发生变化时做出准确的调整.而针对物联网感知层资源有限的问题,文献[42]简化了 XACML,提出了轻量级的 XACML,并给出相应的实施方案.由于 XACML 中采用嵌套递归式匹配方法,计算复杂度较高.文献[43]提出的 XEngine 系统通过将 XACML 策略规则和请求转换为数字表示的形式,减小了 XACML 中嵌套递归式匹配的时间复杂度,提高了策略匹配的效率.但对原始策略进行翻译转化为数字形式时引入的辅助运算数据结构带来了额外的运算量.

ABE 中访问控制策略的表达则通过访问结构(Access Structure)进行描述.访问结构的表达能力是制约 ABE 访问控制技术发展的一个重要因素,关系到整个访问控制系统的效率和保护粒度.

定义 1(访问结构▲).　令$\{P_1,P_2,\cdots,P_n\}$是参与者的集合.对于集合▲$\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$,若 $\forall B,C$:如果 $B\in$▲且 $B\subseteq C$,有 $C\in$▲,称▲是单调的.访问结构▲是$\{P_1,P_2,\cdots,P_n\}$的非空子集.

当前访问结构类型主要可以分为门限、访问控制树及秘密共享机制 3 种.文献[44]首次提出了使用(k,n)门限(Threshold)作为访问控制结构.(k,n)门限结构首先利用拉格朗日插值定理将待发布的秘密信息 s 分为 n 个部分,仅当不少于 k 个信息共同协作时才能重构出秘密 s.如图 4 所示,k_x 表示恢复出秘密信息 x 所需要的阈值,则当 $k_x=1$ 时,门限表示的是或("OR")门;当 $k_x=n$ 时,它表示的是与("AND")门.门限方案优点在于实现简单,系统复杂度较低,ABE 的发展最初也是从门限结构开始的,许多研究都是基于门限结构展开的[5,45-49].但由于门限结构运算单一,只能进行单独的"与"或"或"运算.这种方式仅能简单地反映属性间的数量关系,无法描述属性之间的复杂逻辑关系(如多个"与"和

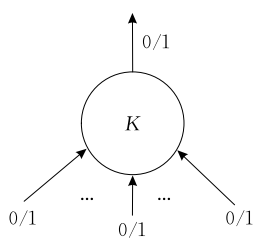


图 4　门限访问结构

① http://xacmlinfo.org/category/xacml/
② http://sunxacml.sourceforge.net
③ http://pythonhosted.org/ndg-xacml/ndg-module.html

“或”的关系的组合),从而不能描述丰富的访问控制策略.

树型访问结构的引入有效提高了访问结构的表达能力[50].如图 5 所示,树型访问控制结构通过对多个“与”、“或”及“门限”操作进行合并,使访问结构能够反映属性间的更为复杂的逻辑关系.设 T 为一树型访问结构,该访问结构中非叶子节点表示一个由其子节点和相应阈值共同描述的门限结构.

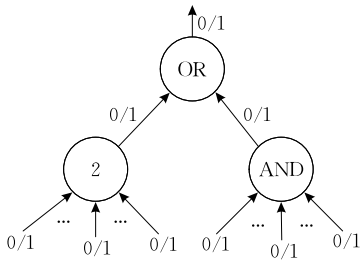


图 5 树形访问结构

叶子节点代表一个相应的属性且 $k_x=1$.当 x 为叶子节点时,与节点 x 关联的属性记为 $attr(x)$.令 num_x 表示节点 x 的子节点的数量,每个节点的子节点从 1 到 num_x 顺序编号.判断属性集合是否满足访问控制树所描述的访问控制策略的方法如下.

设 T 代表一个访问结构树.T_x 表示 T 中以 x 为根的子树,记根节点为 r,则 T 可表示为 T_r.若属性集合 ω 符合 T_x 所代表的访问控制策略,则记 $T_x(\omega)=1$.$T_x(\omega)$ 按下述方法递归进行计算.

(1)若 x 是叶子节点,且 $attr(x)\in\omega$,则 $T_x(\omega)=1$.

(2)若 x 是非叶子节点,令 x' 为 x 的子节点,计算的 $T_{x'}(\omega)$,若至少 k_x 个子节点 x' 有 $T_{x'}(\omega)=1$,则 $T_x(\omega)=1$.

但该结构不支持“非”操作,其表达能力仍然有限.此后,在原有树形结构的基础上通过引入“非”的操作,增强了访问控制树的表达能力[51].然而表达能力的提升增加了密文、密钥的大小,加解密计算复杂度也升高.为了减小计算复杂度,研究者在访问结构中引入了析取范式访问树[52].目前基于树形访问结构的 ABE 机制有很多研究[53-56].树形方案虽然在门限方案的基础上做出了一定的改进,增强了访问结构的表达能力.但同门限方案相同,其在系统初始化阶段需要规定好访问控制系统的属性空间和用户空间的大小,不能满足新型计算环境下用户数量和属性数量动态增长的特点.

为了提高系统的安全性,研究者提出了基于线性秘密共享机制(Linear Secret-Sharing Schemes,LSSS)的访问结构[57].线性秘密共享机制能有效地防止密钥的丢失和恶意用户的攻击,减小秘密共享用户之间的风险和责任.令 $P=\{P_1,P_2,\cdots,P_n\}$ 是秘密共享参与者的集合,$(\boldsymbol{M},\rho)$ 代表访问结构▲($\boldsymbol{M}$ 是一个 $l\times K$ 的矩阵,ρ 为将矩阵中行元素 $\{1,2,\cdots,l\}$ 映射到秘密共享参与者 P 的函数).具体的线性秘密分享方法包含如下步骤:

(1)秘密分享算法.从 Z_p 中随机选取 $k-1$ 个值 $v_1,v_2,\cdots,v_{k-1}$ 与待分享秘密 s 组成一个 k 维的向量 $\boldsymbol{v}=(s,v_1,v_2,\cdots,v_{k-1})$;$\boldsymbol{A}_i$ 为矩阵中第 i 行代表的元素.则秘密参与者 $\rho(i)$ 所获得的秘密共享分量定义为 $\sigma_i=\boldsymbol{A}_i\cdot\boldsymbol{v}$.

(2)秘密恢复算法.若一个秘密参与者的属性集合 $\omega\in$▲,令 $L=\{i\mid\rho(i)\in\omega\}$,则可以根据▲有效地计算出一组恢复系数:$\{\mu_i\}_{i\in L}$,使得 $\sum_{i\in L}\mu_i\cdot\sigma_i=s$.

虽然将访问结构的研究从门限结构、树形结构过渡到更复杂的 LSSS 访问结构可以一定程度上解决系统初始化阶段对属性空间和用户空间大小的要求,但访问结构复杂度的增加也不断增加了系统公钥设计的复杂度,同时增加了系统的计算代价,给采用标准复杂性假设证明系统安全性带来更多的困难.基于属性的加密机制的安全性证明方案通常是基于某个数学难题,目前,常用的数学困难问题包括:离散对数问题和基于格的困难性假设等.虽然基于离散对数问题是传统非量子计算中公认的难题且大量应用在 ABE 研究中,但在量子计算下离散对数问题容易被破解,而量子计算的应用只是时间问题[58],为避免量子时代的密码危机,研究人员提出了基于格的困难性假设.基于格难题的密码设计方案另外一个重要优势在于其较高的运算效率[59].典型基于格的困难性假设可大致分为两类:最短向量问题(Shortest Vector Problem,SVP)和最近向量问题(Closest Vector Problem,CVP)[60].但实际应用中基于格的安全性假设在证明时并不直接规约到 SVP 或 CVP 上,而是规约到小整数解(Small Integer Solution,SIS)问题[61].随着研究的深入,研究者提出了新的规约方法:基于学习误差假设的格安全问题[62].该假设可被规约为最短线性无关向量问题(SIVP)和近似最短向量问题(GapSVP)的最差情况.目前大多数基于格的假设都使用这一方法来证明系统的安全性.同基于离散对数问题等困难性假设相比,基于格的困难性假设可有效地提高系统的安全性.

6 ABAC 中多域合作机制研究

传统的访问控制系统中访问权限的授权任务通

常由单一的授权机构负责.但随着用户和设备数量的剧增,单一授权机构的方式已无法满足访问控制系统对功能和性能的双重要求.此外,随着开放式计算环境的普及,数据在多个机构之间共享和传递日益增多,不同的系统中策略制定规则不同,即使相同的策略在不同的系统中有不同的描述,这都降低了不同域之间策略描述的通用性.访问控制系统面临由单一封闭的环境向多机构协作的方式转换的挑战.保证不同机构之间访问控制策略的正确交互对保证访问控制系统的安全有着重要的意义.

ABAC 中为了协调多个不同域之间的不同的访问控制策略,实现资源的统一的访问控制,需要对不同的访问控制策略进行融合及冲突检测.文献[63]通过将访问控制策略定义为由主体、客体和动作构成的三元组集合,构建了并(addition)、交(conjunction)、差(subtraction)等代数算子用以对不同的策略合成的方式进行抽象,从而实现访问控制策略合成方式的形式化描述.同时该方法具有一定的普适性,为后续的研究提供了基础.但简单的集合的交、并、差等运算无法准确反映真正的合成策略.因此,文献[64]通过属性值的计算结构对文献[63]中提出的策略合成代数进行扩展,提出了基于属性的策略合成代数模型(Attribute-based Access Control Policy Composition Algebra,APoCA).此外,通过将访问控制策略转换为多终端二进制策略树(Multi-Terminal Binary Decision Diagrams,MTBDD)的方法,文献[65]对访问策略进行合并,有效实现了合成代数的演算,为访问控制策略的合成提供了新的解决思路.在此基础上,文献[66]基于 MTBDD 设计了一种策略相似性分析方法.该方法根据用户的查询机制构造策略查询树来进行策略查询分析.而将 MTBDD 同三值逻辑{Permit,Deny,NA}相结合,文献[67]提出了细粒度策略合成代数(Fine-grained Integration Algebra,FIA).但三值逻辑的表达方式较为单一,当出现多个策略需要合作判定时无法描述多个策略之间的关系,仅依据三值逻辑无法做出准确的访问控制决断.针对这一问题研究者们分别提出了基于四值逻辑[68]、六值逻辑[69]或八值逻辑[70]的方法对 XACML 策略以及策略合成的形式化描述方法进行扩展.但 MTBDD 方案中生成的树包含大量冗余路径.为了消除这些冗余路径,基于 BSet 逻辑运算规则,文献[71]提出了一种基于二进制序列集合的策略合成代数算法.该算法具有较强的可扩展性和灵活性,可应用于策略合成、策略分析及冲突检测等多个方面.相比于基于策略树的合成算法,该方法的执行效率有着显著的提高,时间复杂度由 $O(mn \cdot 2^n)$降为 $O(m^2 \cdot n)$(n 为不同的属性约束个数,每条访问控制策略包含 m 个能够输出 Permit 或 Deny 的规则).

ABE 机制采取的策略描述方法同传统的 ABAC 机制不同,针对 ABE 中多域协作带来的挑战,研究者提出了多授权机构下协同合作的 ABE 机制.根据多个属性授权机构之间是否利用一个中央授权机构(Central Authority,CA)进行通信保证密钥和密文的准确性,目前的研究分为:采用 CA 的多机构 ABE 和无 CA 的多机构 ABE 两类.

采用 CA 的多机构 ABE.文献[72]首先提出了多认证机构的属性加密方案(Multi-Authority Attribute-Based Encryption,MA-ABE),在 MA-ABE 方案中,授权机构包括一个 CA 和多个属性授权机构(Attribute Authority,AA).属性通过多个相互独立的 AA 进行管理和认证,之后由 CA 对密钥进行发布.但在该方案中需要一个唯一用户全局标识符(GID)对不同用户进行标注,且 CA 对全部 GID 进行管理,这使得 CA 可以同时掌握系统主密钥和全局标识符,有权解密每个密文,这就要求 CA 完全诚实可信.同时 CA 和全局标识符使得最终的授权仍采用集中式管理方式,与采用多机构分布授权的目标相违背.之后文献[52]通过限定 CA 和各 AA 的功能,将 CA 的功能弱化,并给出了相应的多机构的方案.在基于弱化 CA 可信度假设的基础上,研究者又提出了基于“忠实却又好奇”(honest but curious)的 CA 的方案[73],该方案假设 CA 会按照预先设定的职责行事但也根据自己的兴趣对一些数据进行解密分析.但该方法并不是标准模型下的完全安全方案,同时需要较大的密钥空间扩展,不适用于大规模环境.

无 CA 的多机构 ABE.文献[49]在之前工作的基础上提出了一个改进的无 CA 的多机构 ABE 方案(Improved MA-ABE,IMA-ABE).该方案采用无 CA 的设计思路,去除可信认证机构.同时在 AA 之间引入一个共享的伪随机种子,去除了用户 GID 和解密算法之间的关联,有效地防止属性权威通过计算获得特定用户的信息,增强了多机构 ABE 机制的安全性和在实际应用中的可用性.而通过采用分布式密钥生成协议(DKG)和联合的零秘密共享(JZSS)技术,研究者给出了无 CA 的多授权机构基于属性的加密方案[46].该方案基于 DBDH 假设时

间复杂度较高,效率较低.由于该方案采用了(t,n)门限结构,需要至少有$t+1$个AA是可信的.之后,基于随机预言机模型研究者提出了第一个自适应安全的多机构ABE机制,所提出的方法不需要AA之间相互协作.但是该方法和之前的方法一样都无法支持大规模属性空间的环境[74].

多授权中心允许多个互相独立的属性权威中心共同协作进行属性的管理及密钥的生成,减轻单个授权机构的工作压力.同时多授权机构的机制保证了单个授权机构的失效或遭受攻击不会影响整个系统的安全性.但目前多授权机构的研究主要仍针对有界系统空间的研究,即需预先设定好系统的属性和用户空间.所以设计新型的能够运用到动态大规模计算环境中的多授权机制是今后的研究重点.

7 ABAC中身份认证机制研究

在ABAC机制中,用户权限仅与其属性相关,在隐藏用户的真实身份信息的同时提供有效可靠的访问控制.但正由于这种较强的匿名性,为恶意用户滥用其所拥有的权限带来了方便.拥有不同属性的用户可以通过合谋的方式获取新的属性集合,从而获得新属性对应的权限;恶意用户可以将自己所具有的属性私钥分发给其他属性不满足的用户;属性管理第3方则可以按照访问策略所需求的属性,生成访问全部资源的权限.当这些恶意事件发生时,我们一般无法发觉这些行为,更无法准确关联恶意用户.为了解决这些问题,增强访问控制系统的安全性,构造具有可追踪性的ABAC机制是当前ABAC研究中的一个重要方向和严峻挑战.目前ABAC中对用户身份的认证研究主要集中在两方面:ABE机制中的可追踪机制研究以及基于属性的签名(Attribute-Based Signature,ABS)研究.

根据算法所需输入的不同,ABE机制中的用户可追踪研究可分为白盒追踪方法(White-box Traceability)及黑盒追踪方法(Black-box Traceability).白盒追踪指给定事先设计好的密钥,并将密钥作为追踪算法的输入,从而追踪到设计密钥的用户.而黑盒追踪指仅给定解密设备,无需知道其中封装的解密算法和解密密钥的信息.黑盒追踪算法向该设备提供密文,并从该设备得到其解出的明文,最终达到能够追踪到至少一个参与制造这个解密设备的恶意用户的目的.

白盒追踪ABE机制.文献[75]基于DBDH假设提出了一种白盒可追踪方案(Accountable CP-ABE,CP-A2BE).方案中对每一个ABE用户加入唯一的身份识别属性.在生成用户私钥时,除访问控制策略所需的属性外,需要用户提交相应的身份识别属性.该方案解决了密钥恶意分发和合谋攻击的问题.但是该方案仅支持选择性安全.为了提高白盒追踪机制的安全性和访问控制系统的表达能力,研究者借鉴Boneh and Boyen签名机制提出了一种高效的具有丰富表达能力的可追踪ABE机制,该方案可以支持任意单调的访问结构,同时是自适应安全的[76].

黑盒追踪ABE机制.文献[7]基于DBDH和D-Linear假设提出了黑盒可追踪的KP-ABE方案.该方案在用户私钥中加入唯一标识用户的属性.正常的解密时不需要用户标识属性参与.当运行追踪算法时,通过将用户的标识属性同密文相结合,使得只有具有可疑标识属性的用户才能解密特定的追踪密文,从而判断泄漏密钥的恶意用户.但是该方案不能抵御共谋攻击,如果多个用户共谋生成解密设备则无法判断具体的恶意用户.同时该方案只给出了选择性安全的证明.之后,文献[78]提出了防共谋的黑盒可追踪KP-ABE机制.方案支持任意单调的访问结构,且在标准模型下给出了适应性安全的证明.方案中由可追踪特性所带来的密文密钥的增长仅为亚线性(sub-liner)的,使得所提出的方法具有较高的执行效率.此外,基于DBDH和D-Linear假设研究者提出了一种可追踪CP-ABE方案.该方案中设计了两种不同的加密算法,当使用普通加密算法时,信息的加密中不包含个人标识信息,所有满足访问控制策略的的用户都可以进行解密.而当使用追踪加密算法进行加密时,信息的加密包含被怀疑的用户的个人识别信息,只有满足访问控制规则的被怀疑用户才能对信息进行解密[77].对于用户来说,追踪加密与普通加密算法是不可分辨的,实现了策略的隐藏.但是该机制在保护策略和用户隐私的同时显著增加解密密钥和密文的长度,同时访问结构较为简单,只能表示"与"策略.以上几种ABE机制中的可追踪性研究的比较如表2所示.

结合数字签名的思想,研究者提出了ABS机制[81].数字签名技术的引入保证了用户属性信息的不可否认性、不可伪造性及完整性.ABS机制中签名者声称其签名中包含一组相关属性或满足某种访问控制策略,验证者通过验证签名是否包含相应的属性或满足访问策略对其真实性进行判断.ABS机

表 2　可追踪 ABE 机制对比

可追踪性		针对机制	安全性	是否防共谋	表达能力	系统空间
白盒追踪	文献[75]	CP	选择性安全	是	Monotone	有限空间
	文献[76]	CP	完全安全	否	Any Monotone	无限空间
黑盒追踪	文献[77]	CP	选择性安全	否	Monotone	有限空间
	文献[78]	KP	完全安全	是	Monotone	有限空间
	文献[79]	CP	完全安全	是	Any Monotone	有限空间
	文献[80]	CP	完全安全	是	Any Monotone	有限空间

制能够细粒度地划分身份特征，同时具有很好的灵活性. 之后在环签名(ring signature[82])和群签名(group signature[83])等签名技术的基础上，研究者们提出了改进的 ABS 机制. 在群签名基础上提出的基于属性的群签名方案中，当群成员所具有的属性超过一定的阈值时，可以代表群进行签名，但验证者和群中其他成员无法知晓签名者所拥有的全部属性特征. 但群管理员有权知晓全部成员的属性信息[84]. 而将传统环签名的方法同 ABS 结合所提出的基于属性的环签名方案，利用环签名的匿名性特征保证即使管理员也无法知晓签名者的真实身份[85]. 这些方法中用户可以根据其自身属性向一个可信的属性授权机构请求签名私钥. 但当用户数量和属性数量都非常大时，授权机构的管理和计算负担会非常大，同时降低了整个系统的运行效率. 此外，在面临恶意攻击时这种单一的授权方式无法保证授权机构的安全性，一旦授权系统被攻破，则会导致整个授权系统的崩溃. 因此为了进一步提升 ABS 的实用性及安全性，研究者提出了多授权机构的 ABS 机制. 同多机构 ABE 研究类似，针对 ABS 的研究也可分为基于 CA 和无 CA 两类. 文献[86-87]采用基于 CA 的方式设计了多授权机构环境下的 ABS 机制并给出了相应的安全性证明. 但是同 ABE 机制中的多机构合作类似，CA 的引入使得我们对 CA 必须完全信任，这种假设在真实环境下是不现实的. 因此文献[88]基于无 CA 的方式提出了标准模型下完全安全的分布式 ABS 机制，无需可信 CA，但由于访问结构的限制该方案并不适合大规模环境.

ABS 机制虽然保护了签名者的隐私，但也隐藏了签名者的真实身份. 这一特点使恶意用户可能利用 ABS 的匿名性进行恶意的操作. 因此为了保证签名的安全使用，研究者们提出了可追踪身份的 ABS 方案(Traceable Attribute-Based Signatures，TABS). 通过引入可追踪的思想所提出的可追踪的 ABS 机制在保证签名者隐私性的基础上实现了身份的可追踪性，有效地解决了签名者滥用签名问题. 通过对用户的属性使用比特加密的方法构建签名，研究者提出了可追踪签名者身份的 ABS 机制，并利用非交互证据不可区分方法(Non-Interactive Witness Indistinguishable，NIWI)证明了系统的安全性[89]. 但该方案要求属性权威完全可信且用户及属性权威之间的连接通路是完全安全的，这导致该方案无法应用于实际应用中. 之后文献[90]提出了分布式环境下的可追踪 ABS 机制(Decentralized TABS，DTABS). 但是这些研究需要用户对签名授权机构完全信任，为了降低对授权机构的依赖，在 DTABS 的基础上文献[91]提出减小对中心授权机构的信任的方法，并给出了相应的安全性证明.

虽然引入用户身份可追踪性增加了系统的安全性，但同时也增加了 ABS 安全性证明的复杂度. 同时目前针对 ABS 的研究中访问结构单一，导致其运行效率较低，因此需要考虑利用 LSSS 等较为复杂的访问结构对可追踪身份的 ABS 方案进行改进. 此外，目前大多数机构 ABS 的研究仍采用基于 CA 的方式，对第 3 方授权中心的可信度较为依赖，如何移除可信任中心授权，使多授权中心的 ABS 在实际应用中更具有可行性是今后重要的研究方向.

8　ABAC 中权限更新与撤销机制研究

ABAC 中权限与属性紧密关联，用户属性的变化会导致其所拥有的访问权限发生相应变化. 按照权限管理的粒度，ABE 中的权限管理可以分为 3 类：用户级撤销、用户属性级撤销和系统属性级撤销. 用户级撤销指将用户全部的权限撤销，将其移出访问控制系统. 用户属性级撤销指根据用户属性的变化更新用户所具有的权限，不影响具有相同属性的其他用户. 而系统属性级撤销指更新所有具有该属性的用户. 但无论是哪种粒度的撤销，当属性变化时都需要生成新密钥对与原属性相关的全部数据进行重新加密，这将带来极大的计算消耗. 而新型计算环境下用户和属性的大规模特性和属性权限之间的多对多关系都进一步增加了权限更新的复杂度，给设计有效的权限更新机制带来很大的难度. 按照撤销执

行者的不同,当前权限管理可以分为以下两类:直接管理和间接管理.

8.1 直接管理

直接管理采用人工方式维护用户(属性)-权限列表.最简单的直接撤销方式是将被撤销用户标识的非与密文关联,使得被撤销的用户无法解密相应的密文[51].但是这种方式增加了密文和用户私钥的大小.为了解决密文大小增加的问题,文献[92]提出了一种恒定大小密文的 CP-ABE 方案.但该方案的访问结构较为简单,表达能力较弱.之后结合基于 Broadcast 加密机制,研究者提出了一种属性直接撤销的方案,该方案同时实现了 KP-ABE 和 CP-ABE 上的属性撤销方案.以基于广播密文策略属性加密方法为例,实现形式如下[93].

Setup:输入系统安全参数,生成公钥 PK 和系统主密钥 MK.

Encrypt:输入未撤销用户的用户标记的集合 $S\in U$、用户的访问策略 $A\in$▲、明文信息 M 及公钥信息 PK,输出加密密文 CT.

KeyGen:输入用户标识 $ID\in U$、属性集合 ω、公钥 PK 和系统主密钥 MK,输出用户私钥 $SK_{(ID,A)}$.

Decrypt:输入用户集 s、密文 CT、属性集合 ω、用户私钥 $SK_{(ID,A)}$ 及公钥信息 PK,用户属性满足访问策略则解密信息 M,否则返回错误.

直接管理方式虽然可以实现细粒度的访问控制,但只能实现用户级的管理或采用一次一密(一次加密仅支持一个属性的撤销)的方式实现属性级的管理,无法实现高效的属性-权限之间细粒度的管理.同时由于直接管理方式需要授权机构管理所有用户的权限列表,当用户及属性量很大时,授权机构的存储及管理负担非常大.

8.2 间接管理

为了克服直接管理方式带来的系统管理负担同时实现细粒度的访问权限管理,研究者们提出了间接管理的方法.最早的间接管理方案是通过授权机构周期性地发布更新用户属性所对应的密钥[9].该机制实现简单,但需要与授权机构多次交互.同时,由于密钥定时更新,当有大量密钥同时进行更新时授权机构的运算量会很大.针对密钥多次协商问题,文献[6]通过为每个用户和属性添加一个截止日期,降低了交互次数.上述方法为了保证更新的准确性需要保持用户和授权机构实时在线,针对该问题,文献[94]中提出了一种属性可撤销的 KP-ABE 方案,该方案中,一部分密钥与时间相关,且该密钥由授权机构公布、对全体用户可见,从而消除了密钥更新过程中实时在线问题.上述方法对访问控制策略采取周期性的更新,仅当用户属性对应的失效期到期后才能被撤销.因此这种撤销方式在时间上具有一定的滞后性.虽然这种滞后问题可以通过缩短更新间隔来解决,但更短的更新间隔意味着更新频率的增加,从而间接增加了授权机构的工作量.此外随着系统用户数量增长,授权机构在更新阶段的工作量会急剧增长.

针对这些问题,研究者提出了一些改进方法.文献[95]提出了一种多机构合作情况下的属性撤销方法.通过为每个用户分配一个唯一的 ID 号,当执行撤销操作时,对应的属性权威对 PK 进行更新并对所有未撤销的用户进行广播,实现密钥的更新.同时由于引入多属性权威共同协作的方法,减小了单一属性权威的工作负担.但是该方案需要一个中心权威且完全可信.此外,研究者通过将复杂的密钥更新计算外包给计算能力更为强大的第 3 方机构,以此解决更新滞后问题[8].这种方法实现了密钥的实时撤销,同时不要求授权机构实时在线,从而减轻了授权机构的工作量.但该方案要求第 3 方机构诚实可信.针对该问题,研究者提出了代理重加密方案.通过将 CP-ABE 机制同代理重加密方法相结合,研究者提出了基于代理重加密机制的属性撤销方案.但是并未给出相应的安全性证明和系统的形式化描述[96].在之后的工作中,为了进一步完善已有方案,每个属性被赋予一个特定的 ID 号,同时绑定一个版本号.当需要进行属性撤销时,相应未撤销属性的版本号增加并生成新的 PK 和新的重加密密钥,之后对相应的文件进行重加密[97].但该方案仅能实现属性级的撤销,撤销粒度较粗.在此基础上,研究者基于代理重加密(proxy re-encryption)技术提出了一种 CP-ABE 方案下的属性撤销方法.该方案对系统主密钥的更新信息以及公钥、私钥、代理重加密密钥和密文版本信息进行匹配,只有当用户的私钥版本同对应的密文版本相同时才可解密相应信息.但为了实现实时撤销,代理授权机构需要实时在线[98].而利用条件代理广播重加密的方法将针对某个特定用户组的密文转换为针对多个用户组的密文,从而有效扩展了访问控制策略,同时保证了用户只需利用自身的私钥就可以对密文进行解密,无需生成新的密钥[99].

直接撤销的优点在于仅对需要撤销的用户和属性进行计算,无需对其他为撤销用户进行更新.但也

存在着明显的缺点，在实现整个用户的权限撤销前需要获取用户的详细信息，这使得需要维护一个庞大的用户列表，带来极大的管理负担，目前这种方式很少在大规模数据环境中使用. 同直接方式相比，间接方式无需提前获知全部的用户列表. 但由于将用户权限运算转化为外部计算，相关密钥、数据的交换和访问控制都必须通过一个三方完全信任的第 3 方机构来进行. 但新型计算环境下数据提供者、数据服务商、访问控制授权机构三者之间不可能对对方完全信任，导致原方案中的假设在实际应用中往往是不成立的. 针对第 3 方信任的问题，可以通过将静态或动态的信任模型和访问控制技术相结合，提高访问控制的安全性. 静态信任计算模型可以使用户或者机构在进行数据交互之前计算对其他用户或机构的信任值，并根据相应的信任值计算是否与其进行数据交换或执行相应的访问操作. 而动态信任计算模型如例如 PTM(Pervasive Trust Management)模型[100]、基于 D-S 证据理论的信任评估模型[101]等的引入通过量化计算在数据交互过程中不同用户和机构的行为进行相应信任度的计算，保证交互过程中非正常行为的及时发现，保证了系统的安全性. 同时由于引入了第 3 方机构，密钥和密文在访问控制执行过程中进行多次加解密会导致密文和密钥版本不对应，从而给整个系统的安全带来极大隐患，因此亟需对用户、第 3 方、授权机构之间访问控制策略的同步机制进行研究.

9　ABAC 系统研究趋势

尽管针对 ABAC 的研究已经取得了丰硕的成果，但随着应用环境愈发多样和复杂，ABAC 研究仍然有许多亟待解决的问题.

(1) 为使挖掘出的属性集属性-权限之间的关联关系更符合真实的语义环境，需要引入多属性之间语义关联度的研究. 同时，原始输入中存在的噪音数据很大程度上影响了挖掘结果的准确性，如何解决原始数据中的噪音问题也是值得关注的研究点. 此外，目前的属性-权限关联关系挖掘方法大多使用非负布尔矩阵进行原始权限关联关系的描述，但在实际应用中，定义用户所不能具有的属性有着现实意义，如何将目前的非负关系扩展为包含负属性关系的表达方式及相关的信息挖掘还需要进一步的研究.

(2) 随着应用环境的不断变化，简单的访问结构已经无法满足访问控制系统的安全需求，设计复杂环境下具有丰富表达能力的访问结构是今后 ABAC 中的研究重点. 例如可以利用实际环境中授权机构以及属性之间通常存在层次关系，引入层次化的属性结构，从而使得访问结构的研究具有更强的现实意义. 同时，使用层级属性来优化访问控制结构，可以使得高级别层次节点利用推导算法获取通联关系中所有低级别层次节点对应属性所拥有的权限，大大降低系统复杂度.

(3) 访问控制中的多域合作机制研究是目前新型计算环境下访问控制的研究重点，因此不同域间的策略翻译和融合始终是 ABAC 的研究重点. 不同策略的准确翻译可以保证翻译之后的系统安全性描述等价于翻译之前的描述，为之后的融合和冲突检测奠定基础. 此外，由于不同安全策略的语义表示与理解的不同及策略语言的表达能力不同，会导致翻译之后语义的缺失，从而降低系统的安全性. 如何准确地理解原始策略的语义，同时克服表达能力之间的差异，是多域合作下的访问控制策略融合和系统安全性的重要保障.

(4) 无论是在 ABE 或是 ABS 机制中，用户、数据服务提供商、访问控制授权机构三者之间存在着不同的信任关系. 目前的方案中相关密钥、数据的交换和访问控制都假设通过一个三方完全信任或半可信的第 3 方机构来进行，但这一假设在实际应用中往往是不成立的. 如何减少对可信第 3 方机构的依赖，提升系统的安全性是未来 ABAC 中的重要研究内容.

(5) 目前 ABE 机制的研究大多集中在理论模型研究方面，在云计算、物联网等实际环境中的应用研究还较为缺乏. 例如由于物联网环境存在设备的存储、计算等资源有限等约束条件，使得在物联网环境下利用加密机制有着诸多限制，消除这些限制可以有效地提高 ABAC 的应用范围. 同时 ABE 机制在真实环境下的运行效率及安全性也没有得到验证. 因此需要针对不同的实际环境设计不同的解决方案.

10　总　结

云计算、物联网等新型计算环境下的 ABAC 研究是一个较新的研究方向. ABAC 在有效实现细粒度的非交互访问控制机制的基础上最大程度地保护了用户数据的隐私，具有良好的应用前景. 本文针对

访问控制的准备阶段以及执行阶段面临的挑战系统地分析了目前 ABAC 中的关键技术研究.最后对未来的发展趋势进行了分析与展望.虽然针对 ABAC 的理论研究已取得了丰硕的成果,但其在实际环境中的大规模应用仍面临诸多挑战.希望本文能够为进一步解决 ABAC 中存在的问题提供一定的思路,使 ABAC 能够得真正在实际应用中发挥重要作用.

参 考 文 献

[1] Bertino E, Bonatti P A, Ferrari E. TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security, 2001, 4(3): 191-233

[2] Park J, Sandhu R. Towards usage control models: Beyond traditional access control//Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, Monterey, USA, 2002: 57-64

[3] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Riviera, French, 2010: 62-91

[4] Wang X, Fu H, Zhang L. Research progress on attribute-based access control. Chinese Journal of Electronics, 2010, 38(7): 1660-1667

[5] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 89-98

[6] Bethencourt J, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 2007: 321-334

[7] Yu S, Ren K, Lou W, Li J. Defending against key abuse attacks in KP-ABE enabled broadcast systems. Security & Privacy in Communication Networks, 2009, 19: 311-329

[8] Ibraimi L, Petkovic M, Nikova S, et al. Mediated ciphertext-policy attribute-based encryption and its application//Proceedings of the Information Security Applications. Busan, Korea, 2009: 309-323

[9] Pirretti M, Traynor P, McDaniel P, Waters B. Secure attribute-based systems//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 99-112

[10] Chadwick D W, Inman G, Klingenstein N. A conceptual model for attribute aggregation. Future Generation Computer Systems, 2010, 26(7): 1043-1052

[11] Chadwick D W, Inman G. The trusted attribute aggregation service//Proceedings of the IEEE International Conference on Availability, Reliability and Security. Regensburg, Germany, 2013: 1-27

[12] Lee J, Kim H, Hong J S. An attribute aggregation architecture with trust-based evaluation for access control//Proceedings of the IEEE Network Operations & Management Symposium. Salvador, Brazil, 2008: 1011-1014

[13] Ricci R G, Mesiar R. Multi-attribute aggregation operators. Fuzzy Sets and Systems, 2011, 181(1): 1-13

[14] Nakamura M, Nishimura T, Yamaji K, et al. Privacy preserved attribute aggregation to avoid correlation of user activities across Shibboleth SPs//Proceedings of the IEEE 37th Annual Computer Software and Applications Conference. Kyoto, Japan, 2013: 367-372

[15] Ni Wei-Wei, Zhang Yong, Huang Mao-Feng, et al. Vector equivalent replacing based privacy-preserving perturbing method. Journal of Software, 2012, 23(12): 3198-3208(in Chinese)
(倪巍伟,张勇,黄茂峰等. 一种向量等价置换隐私保护数据干扰方法. 软件学报, 2012, 23(12): 3198-3208)

[16] Li Guang, Wang Ya-Dong. An improved privacy-preserving classification mining method based on singular value decompositio. Acta Electronica Sinica, 2012, 40(4): 740-744(in Chinese)
(李光,王亚东. 一种改进的基于奇异值分解的隐私保持分类挖掘方法. 电子学报, 2012, 40(4): 740-744)

[17] Lee T, Wang H. Attribute extraction and scoring: A probabilistic approach//Proceedings of the 2013 IEEE 29th International Conference on Data Engineering. Brisbane, Australia, 2013: 194-205

[18] Yanen L, Paul H B, Chengxiang Z, Kuansan W. Mining entity attribute synonyms via compact clustering//Proceedings of the 22nd ACM International Conference on Information & Knowledge Management. San Francisco, USA, 2013: 867-872

[19] Huang Jiu-Ming. Research and Implementation on Public Opinion Analysis and Attribute Discovery Oriented Internet Text Mining[Ph. D. dissertation]. National University of Defense Technology, Changsha, 2011(in Chinese)
(黄九鸣. 面向舆情分析和属性发现的网络文本挖掘技术研究[博士学位论文]. 国防科技大学, 长沙, 2011)

[20] Hu Guo-Qing, Li Jian-Hua. A credibility analysis-based method to discover new attributes Web pages. Journal of Computer Technology and Development, 2009, 19(1): 56-59(in Chinese)
(胡国晴,李建华. 一种基于可信度分析的 Web 页面新属性发现方法. 计算机技术与发展, 2009, 19(1): 56-59)

[21] Coyne E J. Role engineering//Proceedings of the 1st ACM Workshop on Role-Based Access Control. Gaithersburg, USA, 1996: 4

[22] Fernandez E B, Hawkins J C, Raton B. Determining role rights from use cases//Proceedings of the 2nd ACM Workshop on Role-Based Access Control. Fairfax, USA, 1997: 121-125

[23] Neumann G, Strembeck M. A scenario-driven role engineering process for functional RBAC roles scenarios: An overview//Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. Monterey, USA, 2002: 33-42

[24] Kuhlmann M, Shohat D, Schimpf G. Role mining-revealing business roles for security administration using data mining technology//Proceedings of the 8th ACM Symposium on Access Control Models and Technologies. Como, Italy, 2003: 179-186

[25] Vaidya J. RoleMiner: Mining roles using subset enumeration//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 144-153

[26] Pletikosa M, Šupica Ž. Database roles analysis using data mining//Proceedings of the Information and Communication Technology, Electronics and Microelectronics. Opatija, Croatia, 2011: 1507-1511

[27] Zhang D, Ramamohanarao K, Ebringer T, Yann T. Permission set mining: Discovering practical and useful roles//Proceedings of the Annual Computer Security Applications Conference. Anaheim, USA, 2008: 247-256

[28] Zhang D, Ebringer T. Role engineering using graph optimisation //Proceedings of the 12th ACM Symposium on Access Control Models and Technologies. Sophia Antipolis, France, 2007: 139-144

[29] Ene A, Horne W, Milosavljevic N, et al. Fast exact and heuristic methods for role minimization problems categories and subject descriptors//Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. Estes Park, USA, 2008: 1-10

[30] Vaidya J, Atluri V, Guo Q I. The role mining problem: A formal perspective. ACM Transactions on Information and System Security, 2010, 13(3): 1-27

[31] Geerts F, Goethals B, Mielik T. Tiling databases//Proceedings of the Discovery Science. Padova, Italy, 2004: 278-289

[32] Frank M, Streich A P, Buhmann J M. A probabilistic approach to hybrid role mining//Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, USA, 2009: 101-111

[33] Molloy I, Chen H, Li T, et al. Mining roles with semantic meanings//Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. Estes Park, USA, 2008: 21-30

[34] Frank M, Berkeley C. Role mining with probabilistic models. ACM Transactions on Information and System Security, 2013, 15(4): 378-397

[35] Guo Q, Vaidya J, Atluri V. The role hierarchy mining problem: Discovery of optimal role hierarchies//Proceedings of the Annual Computer Security Applications Conference. Anaheim, USA, 2008: 237-246

[36] Wang L, Wijesekera D, Jajodia S, Va F. A Logic-based framework for attribute based access control categories and subject descriptors//Proceedings of the ACM Workshop on Formal Methods in Security Engineering. Washington, USA, 2004: 45-55

[37] Cantor S, Kemp I. Assertions and Protocols for the Oasis Security Assertion Markup Language. 2nd Edition. Burlington, Massachusetts, United States: OASIS Standard, 2005

[38] Moses T, Anderson A, Microsystems S, et al. eXtensible Access Control Markup Language. Burlington, Massachusetts, United States: OASIS Standard, 2004

[39] Lang B, Foster I, Siebenlist F, et al. A flexible attribute based access control method for grid computing. Journal of Grid Computing, 2008, 7(2): 169-180

[40] Ray I, Ray I. Trust-based access control for secure cloud computing//Keesook H J, Baek-Young C, Song Se-Jun eds. High Performance Cloud Auditing and Applications, New York, USA: Springer, 2014: 169-188

[41] Liu X, Xia Y, Jiang S, et al. Hierarchical attribute-based access control with authentication for outsourced data in cloud computing//Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Melbourne, Australia, 2013: 477-484

[42] Seitz L, Selander G, Gehrmann C. Authorization framework for the Internet-of-Things//Proceedings of the 14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks. Madrid, Spain, 2013: 1-6

[43] Liu A X, Chen F, Hwang J, Xie T. Designing fast and scalable XACML policy evaluation engines. IEEE Transactions on Computers, 2011, 60(12): 1802-1817

[44] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 457-473

[45] Herranz J, Laguillaumie F, Carla R. Constant size ciphertexts in threshold attribute-based encryption//Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography. Paris, France, 2010: 19-34

[46] Lin H, Cao Z, Liang X, Shao J. Secure threshold multi authority attribute based encryption without a central authority. Information Sciences, 2010, 180(13): 2618-2632

[47] Nali D, Adams C, Miri A. Using threshold attribute-based encryption for practical biometric-based access control. International Journal of Network Security, 2005, 1(3): 173-182

[48] Waters B. Ciphertext-policy Attribute-based encryption: An expressive, efficient, and provably secure realization//Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2008: 53-70

[49] Chase M. Improving privacy and security in multi-authority attribute-based encryption//Proceedings of the ACM Conference on Computer and Communications Security. Chicago, USA, 2009: 121-130

[50] Yu S, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing//Proceedings of the 29th IEEE International Conference on Computer Communications. San Diego, USA, 2010: 1-9

[51] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 195-203

[52] Sascha M, Katzenbeisser S, Eckert C. Distributed attribute-based encryption//Proceedings of the Information Security and Cryptology. Seoul, Korea, 2009: 20-36

[53] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221

[54] Bobba R, Khurana H, Prabhakaran M. Attribute-sets: A practically motivated enhancement to attribute-based encryption //Proceedings of the 14th European Symposium on Research in Computer Security. Saint-Malo, France, 2009: 587-604

[55] Ruj S, Stojmenovic M, Nayak A. Decentralized access control with anonymous authentication of data stored in clouds. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 384-394

[56] Jung T, Li X, Wan Z, Wan M. Privacy preserving cloud data access with multi-authorities//Proceedings of the IEEE Conference on Computer Communications. Turin, Italy, 2013: 2625-2633

[57] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption// Proceedings of the Conference on Computer and Communications Security. Berlin, Germany, 2013: 463-474

[58] Mou Ning-Bo. Design and Security Provement of Public Key Cryptosystems Based on Hard Problem in Lattice [M. S. dissertation]. Xidian University, Xi'an, 2009(in Chinese)
(牟宁波. 基于格困难问题的公钥加密算法的设计与安全性证明[硕士学位论文]. 西安电子科技大学, 西安, 2009)

[59] Wu Yan-Fang. Research of Public-Key Cryptosystems Based on Hard Problem in Lattice [M. S. dissertation]. Beijing University of Posts and Telecommunications, Beijing, 2013 (in Chinese)
(吴艳芳. 基于格困难问题的公钥密码算法研究[硕士学位论文]. 北京邮电大学, 北京, 2013)

[60] Micciancio D, Goldwasser S. Complexity of Lattice Problems: A Cryptographic Perspective. Netherlands: Springer Science & Business Media, 2012

[61] Ajtai M, Jose S. Generating hard instances of lattice problems //Proceedings of the 28th Annual ACM Symposium on Theory of Computing. Philadelphia, USA, 1996: 99-108

[62] Regev O. On lattices, learning with errors, random linear codes, and Cryptography//Proceedings of the 37th Annual ACM Symposium on Theory of Computing. Baltimore, USA, 2005: 1-37

[63] Bonatti P. An algebra for composing access control policies. ACM Transactions on Information and System Security, 2002, 5(1): 1-35

[64] Lin Li, Huai Jin-Peng, Li Xian-Xian. Attribute-based access control policies composition algebra. Journal of Software, 2009, 20(2): 403-414(in Chinese)
(林莉, 怀进鹏, 李先贤. 基于属性的访问控制策略合成代数. 软件学报, 2009, 20(2): 403-414)

[65] Li N, Wang Q, Qardaji W, et al. Access control policy combining: Theory meets practice//Proceedings of the 14th ACM Symposium on Access Control Models and Technologies. Stresa, Italy, 2009: 135-144

[66] Rao P, Lin D, Bertino E, et al. EXAM: An environment for access control policy analysis and management//Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks. Palisades, USA, 2008: 238-240

[67] Rao P, Lin D, Bertino E, et al. An algebra for fine-grained integration of XACML policies//Proceedings of the 14th ACM Symposium on Access Control Models and Technologies. Stresa, Italy, 2009: 63-72

[68] Bruns G, Huth M. Access control via belnap logic: Intuitive, expressive, and analyzable policy composition. ACM Transactions on Information and System Security, 2011, 14(1): 1-27

[69] Ramli C D P K, Nielson H R, Nielson F. The logic of XACML. Science of Computer Programming, 2014, 83(1): 80-105

[70] Ni Q, Bertino E, Lobo J. D-algebra for composing access control policy decisions//Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney, Australia, 2009: 298-309

[71] Liu Chen-Yan, Pan Li, Zi Xiao-Chao. A binary string set based algebraic framework for policy composition. Journal of Shanghai Jiaotong University, 2013, 47: 579-583 (in Chinese)
(刘晨燕, 潘理, 訾小超. 基于二进制序列集合的策略合成代数框架. 上海交通大学学报, 2013, 47: 579-583)

[72] Chase M. Multi-authority attribute based encryption// Proceedings of the 4th Theory of Cryptography Conference. Amsterdam, The Netherlands, 2007: 515-534

[73] Bozovic V, Socek D, Steinwandt R, Villanyi V I. Multi-authority attribute based encryption with honest-but-curious central authority. International Journal of Computer Mathematics, 2012, 89(3): 268-283

[74] Lewko A B, Waters B. Decentralizing attribute-based encryption//Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn, Estonia, 2011: 1-31

[75] Li J, Ren K, Kim K. AABE: Accountable attribute-based encryption for abuse free access control. Cryptology ePrint Archive, 2009, 2009(118): 1-16

[76] Liu Z, Cao Z, Member S, Wong D S. White-box traceable ciphertext-policy supporting any monotone access structures. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88

[77] Li J, Ren K, Zhu B, Wan Z. Privacy-Aware attribute-based encryption with user accountability//Proceedings of the 12th Information Security Conference. Pisa, Italy, 2009: 347-362

[78] Liu Z, Cao Z, Wong D S. Fully collusion-resistant traceable key-policy attribute-based encryption with sub-linear size ciphertexts//Proceedings of the 10th International Conference Information Security and Cryptology. Beijing, China, 2014

[79] Liu Z, Cao Z, Wong D S. Expressive black-box traceable ciphertext-policy attribute-based encryption. IACR Cryptology ePrint Archive, 2012, 2012(669): 1-29

[80] Liu Z, Cao F, Wong D S. Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on eBay//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Berlin, Germany, 2013: 475-486

[81] Maji H. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. IACR Cryptology ePrint Archive, 2008, 2008(328): 1-23

[82] Rivest R L, Shamir A, and Y T. How to leak a secret// Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia, 2001: 552-565

[83] Science C. Group signatures//Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques. Brighton, UK, 1991: 257-265

[84] Khader D. Attribute based group signatures. IACR Cryptology ePrint Archive, 2007, 2007(159): 1-18

[85] Li J, Kim K. Attribute-based ring signatures. IACR Cryptology ePrint Archive, 2008, 394: 1-16

[86] Maji H K. Attribute-based signatures//Proceedings of the Cryptographers' Track at the RSA Conference. San Francisco, USA, 2011: 376-392

[87] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates//Proceedings of the 14th International Conference on Practice and Theory in Public-Key Cryptography. Taormina, Italy, 2011: 35-52

[88] Okamoto T, Takashima K. Decentralized attribute-based signatures//Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography. Nara, Japan, 2013: 125-142

[89] Escala A, Herranz J, Morillo P. Revocable attribute-based signatures with adaptive security in the standard model// Proceedings of the International Conference on Cryptology in Africa. Dakar, Senegal, 2011: 224-241

[90] Kaafarani A El, Ghadafi E, Khader D. Decentralized traceable attribute-based signatures//Proceedings of the Cryptographer's Track at the RSA Conference. San Francisco, USA, 2014: 327-348

[91] Ghadafi E. Stronger security notions for decentralized traceable attribute-based signatures and more efficient constructions// Proceedings of the Cryptographer's Track at the RSA Conference. San Francisco, USA, 2015: 391-409

[92] Zhang Ying-Hui, Zheng Dong, Li Jin, Li Hui. Attribute directly-revocable attribute-based encryption with constant ciphertext length. Journal of Cryptologic Research, 2014, 1(5): 465-480(in Chinese)
(张应辉，郑东，李进，李晖. 密文长度恒定且属性直接可撤销的基于属性的加密. 密码学报，2014，1(5)：465-480)

[93] Attrapadung N, Imai H. Attribute-based encryption supporting direct/indirect revocation modes//Proceedings of the 12th IMA International Conference, Cryptography and Coding. Cirencester, UK, 2009: 278-300

[94] Boldyreva A, Kumar V. Identity-based encryption with efficient revocation//Proceedings of the 15th ACM Conference on Computer and Communications Security. Alexandria, USA, 2008: 417-426

[95] Yang K, Member S, Jia X. Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(7): 1735-1744

[96] Wang G, Liu Q. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services// Proceedings of the 17th ACM Conference on Computer and Communications Security. Chicago, USA, 2010: 735-737

[97] Wang G, Liu Q, Wu J, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security, 2011, 30(5): 320-331

[98] Yu S, Wang C, Lou W. Attribute based data sharing with attribute revocation//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, 2010: 261-270

[99] Chu C, Weng J. Conditional proxy broadcast re-encryption //Proceedings of the 14th Australasian Conference on Information Security and Privacy. Lanzhou, 2009: 327-342

[100] Almen F, Daniel D, Sanch J. Developing a model for trust management in pervasive devices//Proceedings of the 4th IEEE Conference on Pervasive Computing and Communications Workshops. Pisa, Italy, 2006: 267-271

[101] Yuan Lu-Lai, Zeng Guo-Sun, Wang Wei. Trust evaluation model based on Dempster-Shafer evidence theory. Journal of Wuhan University, 2006, 52(5): 627-630(in Chinese)
(袁禄来，曾国荪，王伟. 基于 Dempster-Shafer 证据理论的信任评估模型. 武汉大学学报，2006，52(5)：627-630)

FANG Liang, born in 1989, Ph. D. candidate. His research interests include IoT security, access control etc.

YIN Li-Hua, born in 1973, Ph. D., associate professor. Her research interests include network security, security evaluation etc.

GUO Yun-Chuan, born in 1977, Ph. D., associate professor. His current research interests include security evaluation, formal methods and IoT security.

FANG Bin-Xing, born in 1960, Ph. D., professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His current research interests include network security and information content security.

Background

Access control, being at least three decades old has attracted extensive attention from both academia and industry and widely been used in industry to prevent unauthorized access. However, the traditional access control fails in some emerging computing paradigms (e. g. cloud computing, IoT computing and social computing) because of the characters in these paradigms like heterogeneity, dynamism, large scale and multi domain.

To solve these problems and guarantee that access is authorized in new paradigms, many efforts have been spent on designing new access control technologies over recent years. During these works, Attribute-based Access Control (ABAC), which introduced attribute into access control to achieve fine-grained control, has been followed by the increasing numbers of conference publications and journal articles. In this paper, we summarized the key technologies in the ABAC schemes including the attribute engineering technologies and the Attribute-Based Encryption which ensured fine-grained access control while achieving both data confidentiality and identity privacy. Then we discussed the open areas and unresolved challenges. Finally, possible future works and some conclusions are pointed out.

This work is supported by the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA06030200), the National High Technology Research and Development Program 863 (Grant No. 2013AA014002).