基于 ABAC 的企业云存储访问控制研究与实现

作者：梁科

云存储服务可以方便地为人们提供数据的存储和数据共享服务，但同时也带来了新的访问控制问题。尤其是在企业云存储环境中，用户的访问控制需求具有多样性和动态变化的特点。然而传统的访问控制方法难以解决云环境下复杂的访问控制问题。

针对企业云存储中企业用户的访问控制需求，在 ABAC(Attribute-based Access Control，基于属性的访问控制)模型的基础上进行扩展，提出了一种适合企业云存储的细粒度访问控制模型。模型中引入主体身份属性、主体业务属性、身份与业务属性关联、主体上下级关系、主体的权限受限继承、客体域标签属性、义务状态等概念，并对这些概念进行了形式化描述。扩展后的模型具有细粒度和动态访问控制等特点，能够满足企业灵活和动态变化的访问控制需求，同时适用企业中用户分级管理。采用标准的访问控制描述语言 XACML(Extensible Access Control Markup Language)来表达属性访问控制策略和请求，支持多种逻辑表达式和属性类型，具有很强的策略表达能力，同时具有可扩展性。针对 XACML 缺乏冲突策略检测的能力，设计了一种策略冲突检测方法，可以有效检测出冲突的策略，并且保证了策略评估的安全性、一致性。最后，在 OpenStack 云存储架构基础上对扩展的模型进行了实现，并以校园云存储系统为应用案例，对云存储的访问控制功能进行测试，测试结果表明该模型能够实现细粒度的、灵活的访问控制，保证了数据的隔离和共享安全。