

工程成果	密文云存储系统 (PCloud)
申请人	陈驰
团队成员	田雪、于晶、杨腾飞、王朝刚、朱晓杰、申培松、李丹、王万乐、陈盛
申请人自述	<p>目前的云存储模式中，云服务提供商通常采用明文形式存储数据并且缺乏不同用户数据之间的隔离机制，一旦云服务提供商遭到攻击，脆弱的防护机制将导致大量用户数据的泄漏。数据所有权和管理权分离，作为数据所有者的用户不再拥有数据管理权，云服务提供商可以完全控制用户数据。如何保护用户数据隐私、防范云服务提供商对用户数据的滥用已成为一个重要的安全挑战。</p> <p>针对上述问题，可采用先加密数据再同步到云端的存储模式，但数据加密混淆了数据之间的顺序关系，使得索引失效，检索变得困难。</p> <p>本项目基于加密存储的思想，以云计算环境中密文数据检索为关键技术，研发了基于 HDFS 服务器端以及 Windows 和 Android 平台的客户端的密文云存储系统。该系统中，用户数据在终端存储、传输过程和云端存储均为密文形式，用户通过控制密钥掌握数据的管理权，可有效的防止云服务商以及恶意第三方对数据的窃取，即使终端丢失或云端受到攻击，用户存储的密文数据仍然不会泄露隐私信息。密文云存储系统具有以下特色：</p> <ol style="list-style-type: none"> <li>1、跨终端的统一数据视图：同时支持 Windows 和 Android 桌面，为用户提供不同终端上的统一数据视图。</li> <li>2、数据加密对应用层透明：数据加解密过程对上层应用透明，用户在使用中感受不到加解密过程的存在。</li> <li>3、全生命周期的数据加密保护：数据在终端、传输过程中和云端都以密文形式存在，全面的保护了数据安全性。</li> <li>4、支持文本文件的检索：提供文本文件的密文索引，可依据用户提供的关键词查找相关文档，并且不会向云端泄露文档或关键词内容。</li> <li>5、支持云平台扩展：分布式文件系统可采用基于 HDFS 的私有云存储模式，也可对接第三方云存储系统。</li> </ol> <p>系统目前已发布 2.0 版本，现正面向公众提供免费的密文云存储服务，发布网址：<a href="http://pcloud.sklois.cn">pcloud.sklois.cn</a>。于此同时，PCloud</p>

	<p>系统已在新疆云计算中心部署应用，结合电子政务应用为用户提供文件的密文存储，取得了良好的应用效果。与中央人民广播电台的合作也在洽谈之中，预计将很快在广播行业用于节目的安全存储。</p>
--	------------------------------------------------------------------------------------------------