面向 P2P 社交网络的自主授权 CP-ABE 原型系统的设计与实现

作者：文子龙

随着社交网络的发展，越来越多的人使用社交网络进行信息发布、结交朋友、买卖商品、寻找工作等活动。社交网络给人们生活带来了便利，也给互联网内容带来了多样化和个性化。目前的社交网络应用都是基于 C/S（Client-Server，客户端-服务器）架构，在这种架构模式下，用户的个人数据都是保存在社交网络服务运营商的服务器上，用户对其数据失去了直接的控制权，必须依赖服务器来保证数据的安全性，如果服务器没有采取有效的安全措施，这些真实性很强的数据可能会被未授权用户查看，也可能会被恶意用户窃取。此外，一些运营商可能出于某种利益上的原因将用户的全部或者部分数据提供给第三方导致用户个人数据的泄露。

为了解决用户个人数据在服务器上存在的安全隐患，设计和实现了一款在 P2P 架构模式下的社交网络应用原型系统。在该系统中用户的个人数据保存在本地，由用户进行自主管理，同时结合属性基加密的方式让用户可以对数据制定灵活的访问控制策略，从而控制数据的共享范围，而且加密的方式也保证了数据在传输过程中的安全性。此外系统还使用了 BitTorrent 协议来对网络中文件进行传输，保证在网络节点处理能力不强，带宽资源有限的情况下也能够实现社交网络中对文件的共享功能。

最后对实现的原型系统进行了评估。实验结果表明，在 P2P 架构下的社交网络应用中，用户对其自身的数据具有更好的控制性，能够有效的防止个人数据泄露的风险。