# 云数据持有性审计研究与进展

田晖[1] 陈羽翔[1] 黄永峰[2] 卢璇[3]

[1]华侨大学计算机科学与技术学院，厦门 361021 [2]清华大学电子系，北京 100084

[3]华侨大学网络技术中心，厦门 361021

## 前言

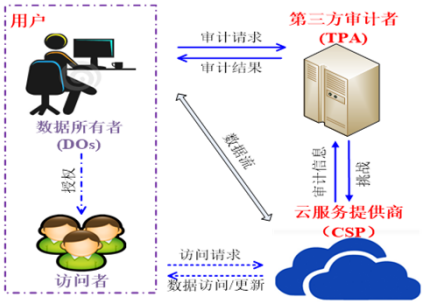
云存储以其高性能和低成本等优势吸引了广泛的关注，但云存储服务提供方无法获得用户信任的现状正阻碍着云存储的推广与发展。为应对该挑战，以相关密码学理论为支撑，以云数据安全性与完整性（持有性）的远程验证为目标的云数据安全审计技术应运而生，并在近来得到了长足的发展。

## 审计目标

- 云数据持有性审计方案应能有效的抵抗取代攻击、重放攻击、伪造攻击等一系列云服务方的不诚信行为。
- 在审计特性或审计功能上各有侧重。
- 在确保审计结果正确性的同时，审计方案应尽可能减少计算和通信开销。

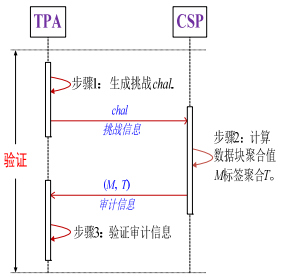
## 审计模型

公开审计通过引入可信第三方，增强审计结果的可信性和权威性，并同时可以减轻用户负担。基于第三方的公开审计模型已成为云数据持有性审计的发展趋势。




云数据公开审计模型图

## 审计基本方案

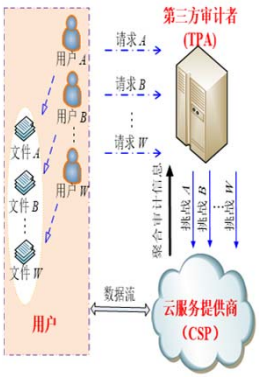



公开审计模型图

基于同态认证技术的审计方案，其思想是：用户为每个数据块生成不可伪造的同态标签，并随数据块一同传送到云服务方上存储。

## 批量数据审计

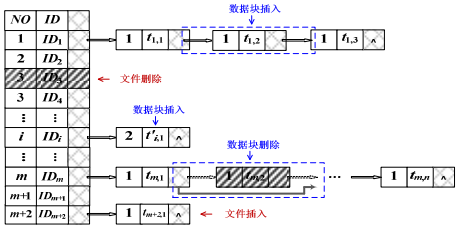
当同时收到来自多个用户的审计请求时，常采用批量审计方法，即利用同态标签的可聚合特性，将不同审计请求产生的审计证据聚合后再一次性完成验证。




批量审计模型图

## 动态数据审计

基于动态数据的审计方案不但要能够适应其数据的频繁更新，还需确保数据新鲜度。将认证数据结构与审计算法相结合是实现动态数据审计的有效途径。




认证数据结构图

## 共享数据审计

针对共享数据的审计方案不仅需要保证数据的完整性，还需考虑用户组的管理（一旦有用户退出，所有涉及其签名的数据块标签需要重新生成)和用户的个人隐私保护（涉及数据内容本身的隐私以及用户的行为隐私）等问题。

## 未来的工作

未来云数据持有性审计研究仍存在着如下挑战或有待进一步探索的问题:

- 动态数据审计方案需要被更加的完善,如支持细粒度更新的数据完整性审计。
- 快速准确地定位出错的用户文件（或副本文件）仍是批量审计（多副本审计）中一个尚待解决的开放问题.
- 更完善和高效的多用户共享数据持有性审计是未来仍需探索的方向之一。
- 为提高审计效率，针对多媒体数据活跃度较小但体量大的特点，提出一种可逆透明水印的公开审计方法。
- 根据云存储服务和大数据应用的发展需要，细分数据类型，进而提高审计效率；从审计系统的实际应用出发，建立可扩展的大数据持有性审计模型，实现多种不同审计方法之间的信息互补和功能协作。

**联系方式:**
**华侨大学网络信息安全实验室**
**Tel: 0592- 6162552**
**Email: htian@hqu.edu.cn**