一种支持多粒度数据完整性的灵活认证方案

关键词：云计算；数据完整性；粒度签名动态操作（Granularity Signature Dynamic operation）；

摘要：为了扩展数据完整性验证方法的灵活性，适应不同的验证环境，本文提出了一种可以支持多粒度的改进方案。它将文件组织成三种粒度，如数据块，数据子块和基本块，基本块实现数据采集，形成数据子块。登录数据子块，使用子块的签名生成块的签名。 改进程序可以实现数据块和子块的验证。 验证数据块可以减少验证过程中的数据流量，两个粒子组合可以提高整体效率。在提出的分层merkel哈希树中，子块或子块可以支持动态操作。通信性能分析表明，改进方案有效，具有较好的实用性。

介绍：数据完整性已成为云存储领域的主要安全威胁之一，Ateniese等[1]提出了用于初始数据完整性验证程序的PDP模型，Erway等[5]提出了一种支持全动态数据更新的协议，Kaliski [7]是第一个在他们的模型中考虑POR程序的人。

在验证中，C.Wang等[3] [4]使用MHT作为验证结构，使用数据块标签作为认证的基本数据，通过数据块签名绑定数据块及其标签，但C.Wang对应的BLS[6]签名要求固定块大小，仅适用于较小的数据块验证，在认证过程中导致过多的通信，效率不高。本文结合文献[8]中提到的不同粒度的思想，提出了基于两种粒度的数据安全认证方案，提出了一种更加灵活的认证模式。在云环境下，验证的粒度不是越大越好，粒度越大可以减少流量，但粒度越小，提高验证效率。本文针对这两种细粒度[2]的数据块和子块，在云环境中验证操作更频繁，因为流量要求相对较低的情况，验证者可以选择验证子块单元，而在流量要求更严格的环境中，验证者可以通过块进行验证。它可以提高验证的整体效率，增加验证的灵活性。同时提出一种分层的merkle哈希树，两种粒度可以动态插入，删除和更新，对于用户的威胁，它增加了服务器验证根节点，确保实时的错误检测和安全性，确认用户提交数据文件，元数据，签名过程的准确性。它还可以支持隐私和公共可验证性。

相关概念：

1. 同态线性认证

对于每个数据块mi，任何挑战值chal = {i，vi}i∈I，I = {s1，...，sc}由验证者发送，服务器可以同态建立验证标签值μ=Σi∈Ivimi

B. 双线性配对

设G1，G2为两个加法组，GT为乘法循环组，顺序为素数P.u和v分别是G和G的发生器。双线性配对有以下属性：1）双线性:对于，且，和也 。 2) 高效的可计算性：取任何，存在一个有效的算法。3）非退化：取任何，存在

拟议方案：

定义1：假设子块签名可以表示为块签名可以表示为，其关系为：

定义2：设表示块标签，表示子块标签，其关系为：

1. 分层MHT

分层MHT。它是MHT逻辑上的层次结构划分。其目的是生动展示完整性检查过程中两种粒度类型，并支持动态子块和块的操作。 分层MHT结构可以如图1所示，树分为两层，I层和J层。下面的虚线是J层，J层的叶节点表示子块标签的散列值。虚线上方是I层，I层的叶节点表示块标签的散列值。j层根散列值是i层叶节点的散列值。

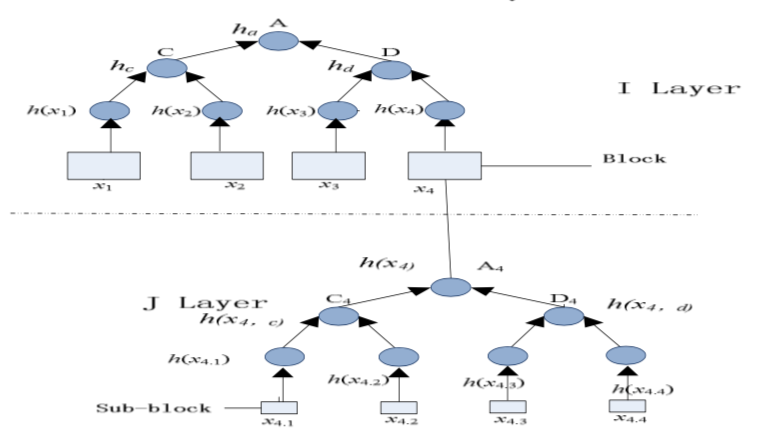


图1

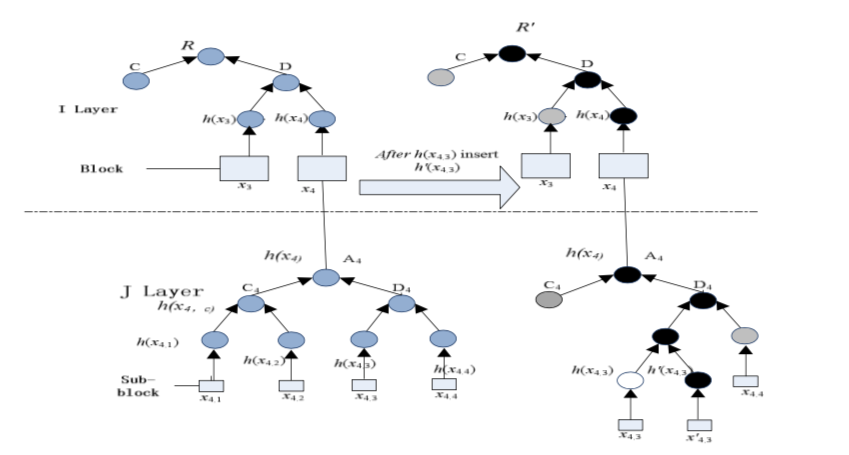


图2

B.数据完整性验证协议

建立阶段:(生成密钥;生成文件标签;生成认证标签;)

生成密钥：用户运行keygen算法生成公钥和私钥，首先用户可以从G1中随机选择一个签名（spk、ssk）、随机数和随机选择k元素，顺序；计算v=ga，然后生成私钥sk（a、ssk）和公钥。sk由用户保留，pk释放给TPA和CSS。

生成文件标签：给定文件，，,文件F的标签是t，