DOI:10.13718/j.cnki.xsxb.2020.09.019

# 基于双服务器 PEKS 框架的高效云存储系统①

黄峰亮[1], 钱晓捷[2]

1. 郑州铁路职业技术学院 实践教学中心, 郑州 451460;
2. 郑州大学 信息工程学院, 郑州 450001

**摘要:** 为降低云存储用户成本并提高安全云存储效率, 设计了一种多用户并发的云存储系统, 提出基于双服务器关键字搜索的公钥加密(Public Key Encryption with Keyword Search, PEKS)搜索框架. 设计的云存储系统通过存储引擎动态策略可以在多种存储方法之间自由切换, 使用硬件负载平衡、中间缓冲和 First－move First－failure 策略来应对大量用户访问, 提高请求响应率和系统稳定性; 并行 Master / Workers 模式有效处理单个大文件请求, 通过令牌机制进行文件传输恢复和并发传输. 所提的双服务器 PEKS 搜索框架通过设计的线性同态平滑投影 hash 函数, 使得所提搜索框架具有更高的安全性, 解决传统 PEKS 的安全漏洞. 实验结果表明, 所提方案可以防止内部关键字猜测攻击, 且其平均响应时间和计算效率优于现有其他方案.

**关 键 词:** 多用户并发; 关键字搜索; 双服务器; 平滑投影 hash 函数; 云存储系统

**中图分类号:** TP391 **文献标志码:** A **文章编号:** 1000－5471(2020)09－0124－08

随着云计算的日益普及, 云存储成为虚拟化环境的理想存储方式, 与传统的存储设备相比, 云存储不仅仅是一个硬件, 而且还是一个由网络设备、存储设备、服务器、应用程序、通用访问接口、接入网络和客户端程序组成的系统[1]. 云存储吸引了许多信息服务供应商的大量支持和关注, 典型的代表是 Dropbox, Amazon S3, 百度 Netdisk, 腾讯微盘, 华为网络盘等[2]. 当前的云存储主要基于公共云存储, 但该技术尚未完全普及, 因为用户对没有保密协议的公共云存在怀疑, 且企业用户与供应商合作的成本较高. 目前的云存储厂商大多依赖硬件, 跨平台较弱, 存储介质单一, 即使存储系统有大量数据, 它也没有相应的大数据挖掘服务. 因此, 低成本和多功能的安全云存储系统受到越来越多的关注, 宋衍等[3]提出了支持安全共享的云存储系统, 通过对称加密、属性加密和代理加密的融合, 实现加密保护、访问控制和高效检索. 刘毅文等[4]设计了基于 Docker 的轻量级云存储系统, 该系统具有较高的性价比, 能够很好地满足用户对低成本、高效、数据可靠的云存储需求. Chen 等[5]提出一种弹性云存储系统, 可以根据大数据应用的实时需求动态扩展/缩小存储系统, 同时采用一种基于数据块的新型复制方案, 对存储系统中的数据进行细粒度的维护.

除了成本和可用性, 云存储的安全也是云存储的主要挑战, 由于数据安全问题, 一些企业拒绝在云中存储敏感数据[6]. 数据所有者可能无法完全控制其在云中的数据, 因此他们可能会担心数据会被攻击者访问或篡改. 此外, 云服务提供商也可以访问用户的个人数据[7-8]. 对于普通用户而言, 云存储的性能和效率也是影响他们迁移到云的重要因素[9]. 为解决云存储安全问题, 许多研究人员提出了自己的算法和解决方案, 任鑫垚等[10]提出了基于密钥策略属性加密的云存储安全框架, 用基于密钥策略属性加密的方法对数据进行加密, 增强数据的安全性. 王少泫[11]通过对云存储系统加密方法的研究, 提出一种基于封闭环境加密的云存储方案(Closed-Box Cloud Storage, CB-CSS), 能阻止操作系统中的不良应用以及云管理员的攻击,

① 收稿日期: 2019－08－14
基金项目: 河南省科技厅基础与前沿技术研究计划项目(152300410191).
作者简介: 黄峰亮(1980－), 男, 硕士, 实验师, 主要从事计算机应用研究.

有效防范数据泄露. 但是，这些加密方法在应对新应用时存在不足，如密文数据的搜索问题，因此研究者提出了带关键字搜索的公钥加密(Public Key Encryption with Keyword Search，PEKS)云存储方案，如不可伪造的可搜索加密审计日志方案[12]，但是已有方案都是传统的公钥加密体制，存在证书管理等问题，因此后来的研究者提出了改进的 PEKS 搜索方案. 徐海琳等[13]提出无双线性对的带关键词搜索方案，解决复杂证书管理问题. Suzuki 等[14]给出了 SCF-PEKS/PKE 的正式安全定义，并提出了基于匿名身份加密和基于标签加密的 SCF-PEKS/PKE 通用结构. 但是，这些 PEKS 框架中采用的云存储系统都是针对公共云存储资源的.

本文针对现有云存储系统的高成本和安全性问题，设计了多用户并发的安全云存储系统，提出了基于双服务器 PEKS 的搜索框架. 本文云存储系统，通过分层网络减少存储攻击，采用引擎动态策略，可以自由切换系统运行不同的存储引擎，然后通过一系列算法和策略实现多用户和大文件的高效处理，同时降低开发成本. 通过双服务器 PEKS 搜索框架，能够解决关键字猜测攻击等问题，进一步保证云中用户数据安全. 实验结果表明，本文所提方案可行且有效.

## 1　多用户并发云存储系统

针对云存储用户多、输入/输出(Input/Output，IO)密集的特点，对分布式存储系统的各个模块进行设计，采用并行 Master/Workers 模式实现大数据的并发读写. Master-Worker 模式是一种常用的并行模式，其核心思想是系统由 Master 进程和 Worker 进程协作工作. 接收和分配任务由 Master 进程负责，处理子任务由 Worker 进程负责. 当子任务处理完成后，每个 Worker 进程将结果返回给 Master 进程，并由 Master 进程汇总，得到系统的最终结果. Master-Worker 模式具有 2 个明显的优势：①提高系统吞吐量，②系统请求者不用等待任务处理. Master-Worker 模式将一个大任务分解成若干个小任务并执行；当任务提交后，Master 进程会分配任务并立即返回，该处理过程是异步进行的，因此系统请求者不会出现等待现象.

云存储系统的结构分为 4 层：外部网络层、代理层、业务逻辑层和数据层. 为了保护系统安全，数据和业务在逻辑上是分开的，即每层之间只允许自上而下的访问，而禁止反向访问，结构图如图 1 所示.

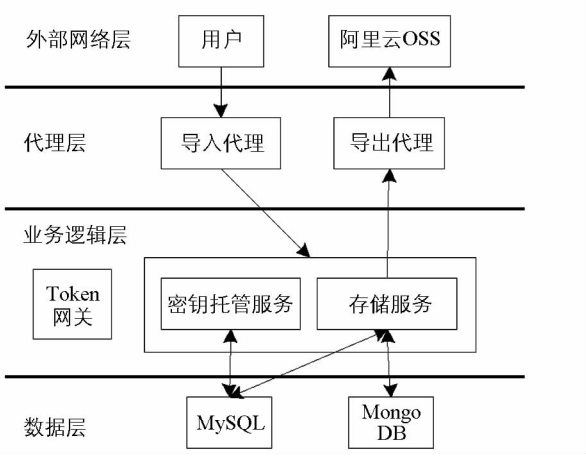


图 1　云存储系统分层网络结构

外部网络层：客户端和第三方服务部署在外部网络层，出于安全考虑，只有通过防火墙和加密的 HTTPS协议才能使外部网络层中的所有组件访问云服务.

代理层：代理层主要负责接收和发送用户的请求，主要由导入代理和导出代理组成. 导入代理主要负责用户请求的安全认证、缓冲和统计. 用户请求不直接进入逻辑层，首先进行令牌验证，不符合要求的请求将被过滤掉，从而避免大部分 DDOS(Distributed Denial of Service，DDOS)攻击. 即使代理层受到攻击，也无法知道业务逻辑和用户数据. 此外，攻击两层的概率非常小，图 1 中分层的存储结构增强了云服务的安全性.

业务逻辑层：作为云服务的核心，该层提供所有业务逻辑服务，如帐户服务、文件存储服务、支付服务、管理控制台和目录服务等. 所有服务都通过非加密的 HTTP(Hyper Text Transfer Protocol，HTTP)请求相互访问，以加快处理速度.

数据层：作为敏感信息，数据部署在底部，包括关系数据库和 NoSQL 数据库，以及文件存储服务使用的文件系统. 数据层的安全性和性能尤为重要，因此该层采用了分区和集群方法.

### 1.1　多用户大规模缓冲缓存方法

由于云计算服务的技术挑战主要来自大型用户集群，高频率并发访问和海量数据，当任何简单的业务需要处理千兆字节的数据和数十亿的用户时，现有云存储系统效率降低，缓冲缓存方法可以分发大规模的

用户访问，改善用户体验，保证系统在大规模访问时不会崩溃. 缓冲缓存方法包括负载均衡、队列缓冲和First-move First-failure策略.

对于负载均衡，随着云服务中高并发性和海量数据访问的增加，可以通过添加更多的服务器来分担原始服务器的访问和存储压力. 负载平衡调度设备可以将用户的请求分发到每个应用服务器集群，如果有更多的用户，集群中将添加更多的应用程序服务器. 在所提方案中采用了硬件负载平衡调度，可部署在任何应用服务器之上. 用户的访问由负载平衡设备进行调度，然后以相对较小的负载发送到服务器进一步处理.

队列缓冲选用Active MQ作为缓冲区来完成保护暂停模式，在频繁的客户请求中，消息队列充当中间访问并存储挂起的请求，当服务器进程完成时，会立即从队列中提取客户端请求.

First-move First-failure策略的核心思想是，当出现大量请求时，随机选择部分请求并直接返回失败，从而使已批准的请求在应用程序可承受范围内. 对于失败的请求必须有重试机制，根据概率理论，所有$n$个请求的失败概率都很低，不会出现用户一直失败的现象，保证了系统的稳定运行. 如备份客户端是客户端应用程序之一，由于备份客户端是IO密集型应用程序，因此只能在没有前端操作时执行后台操作. 通常，最频繁的备份启动发生在4:00－10:00之间. 系统将应用程序接口(Application Programming Interface，API)层中的通过率阈值设置为默认值100%. 当并发请求超过系统限制时，将向下调整阈值，使系统只能处理70%的请求，其他请求将被直接拒绝，并显示“系统忙”状态.

### 1.2 业务层逻辑操作

业务层实现了关键业务逻辑操作，包括安全认证，存储引擎的初始化与切换、文件传输及恢复等操作. 通过使用OAuth 2.0软件实现安全认证，允许用户提供令牌来访问存储在特定服务提供商中的数据.

为了满足不同企业或同一企业不同部分对云存储不同的要求，如安全性和存储成本等，本文设计了一个运行时可在不同企业或部门之间自由切换的存储引擎，引入一种存储引擎动态策略模式(图2).

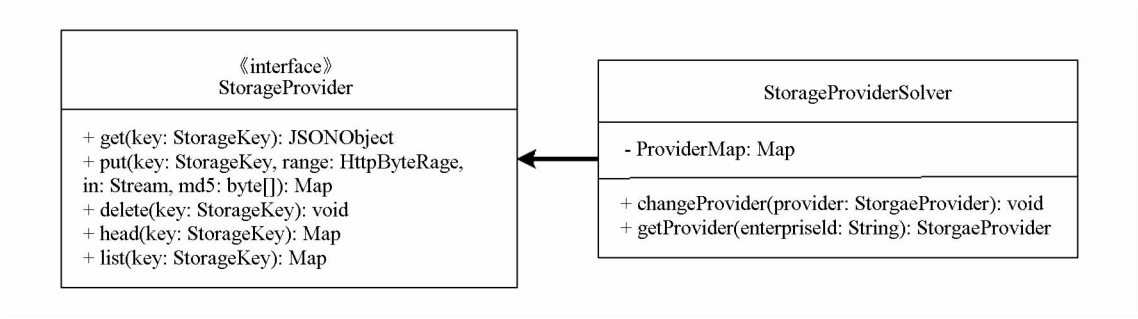


图2 存储引擎动态策略模式类图

不同存储引擎在StorageProvider接口中可实现该方法. 在运行时，调用StorageProviderSolver类中的方法changeProvider()和getProvider()，根据不同参数在不同的存储引擎之间自由切换.

文件操作中使用加速大文件上传的Master/Workers模式，能够在文件上传/下载失败时提供恢复令牌，最终完成上传/下载任务. 如果文件上传或下载失败，用户将尝试重新传输文件，为了避免从头开始重传，需要对传输文件进行恢复. 在上传文件之前，首先计算文件大小和校验和，计算的信息被粘贴在请求报头中并发送到服务器，服务器接收文件并将其存储在临时文件夹中. 完成传输后，使用上传文件的大小和校验和来确定文件是否完成，如果未完成，将生成恢复令牌，当客户端发现上传失败时，将启动重传过程并调用API以获取恢复令牌，恢复令牌和用户身份验证令牌一起提交给服务器，服务器将验证恢复令牌并重新传输未完成的文件. 重复此过程，直到校验和一致且文件上传完成.

### 1.3 数据层和部署

本文云存储系统中数据库和文件存储保存在图1数据层中，其中的数据只能由业务逻辑层访问，极大地提高了数据的安全性. 数据层使用MongoDB的NoSQL和传统的关系数据库MySQL. 非关系数据库以键值对存储，其结构不固定，每个元组可以有不同的字段，并根据需要增加自己的键值对，具有易于扩展、数据量大、性能高、数据模型灵活、可用性高等特点. 在本文系统中，对存储引擎表、元数据表和许可证表

进行了密集的操作，由于客户需求的不断变化，表的结构也在频繁地变化. 对于部署管理，由于多个客户端可能在同一个表上操作，并且以后可以通过用户的额外付款来扩展存储部署，因此事务处理需要一致. 存储引擎表、元数据表和权限管理表存储在 MongoDB 中，部署表存储在 MySQL 中.

本文云存储系统中部署分为数据中心集群、服务器集群(数据中心)和虚拟机，作为云服务的一部分，系统部署在数据中心集群中. 在云服务中，位置服务将多个数据中心相互关联，改变了用户终端服务的域地址. 服务器集群构成一个数据中心，在单个数据中心里，网络分为 3 层(除外部网络层)，如图 1 所示每层中的服务只能是向下或横向的. 向上访问需要一个特殊的代理接口，每个服务都由服务器集群组成. 服务器通过负载平衡器连接.

为了提高硬件利用率，每台服务器由 4 台虚拟机组成，可以为每个虚拟机分配不同的 IP 地址并安装不同的软件. 采用部署管理应用程序，可以预先读取开发人员编写的配置脚本，并配置和释放负载平衡，应用服务器和数据库，解决了多个虚拟机安装许多不同软件的问题.

## 2　云存储系统中双服务器 PEKS 搜索框架

### 2.1　双服务器 PEKS

双服务器 PEKS 由(KeyGen，DS-PEKS，DS-Trapdoor，FrontTest，BackTest)组成，KeyGen 算法用于生成前端和后端服务器的公钥/私钥对. 陷阱门生成算法 DS-TrapDoor 是公开的，而在传统 PEKS 中 TrapDoor 算法以接收者的私钥作为输入，这是由于这 2 个系统所使用的结构不同造成的. 在传统的 PEKS 中只有一台服务器，如果陷门生成算法是公共的，那么服务器可以对关键字密文发起猜测攻击，然后恢复加密的关键字，因此不可能实现用户数据安全. 在双服务器 PEKS 框架下，当公开陷门生成算法时，通过 2 个独立的服务器运行测试算法 FrontTest 和 Backtest，实现云存储的语义安全性. 双服务器 PEKS 框架中各部分算法定义如下：

1) Setup($1^{\lambda}$)，以安全参数 $\lambda$ 为输入，生成系统参数 P；

2) KeyGen(P)，以系统参数 P 作为输入，分别输出前端服务器的公钥 / 密钥对($pk_{FS}$，$sk_{FS}$)和后端服务器的公钥 / 密钥对($pk_{BS}$，$sk_{BS}$)；

3) DS-PEKS(P，$pk_{FS}$，$pk_{BS}$，$wk_1$)，以前端服务器的公钥 $pk_{FS}$、后台服务器的公钥 $pk_{BS}$ 和关键字 $wk_1$ 作为输入，输出 wk 的 PEKS 密文 $CT_{wk_1}$；

4) DS-Trapdoor(P，$pk_{FS}$，$pk_{BS}$，$wk_2$)，以前端服务器的公钥 $pk_{FS}$、后台服务器的公钥 $pk_{BS}$ 和关键字 $wk_2$ 作为输入，输出陷门 $T_{wk_2}$；

5) FrontTest(P，$sk_{FS}$，$CT_{wk_1}$，$T_{wk_2}$)，以前端服务器密钥 $sk_{FS}$、PEKS 密文 $CT_{wk_1}$ 和陷门 $T_{wk_2}$ 作为输入，输出内部测试状态 $C_{ITS}$；

6) BackTest(P，$sk_{BS}$，$C_{ITS}$)，以系统参数 P、后台服务器密钥 $sk_{BS}$ 和内部测试状态 $C_{ITS}$ 作为输入，输出测试结果 0 或 1；

对于任何关键字 $wk_1$，$wk_2$ 和 $CT_{wk_1} \leftarrow$ DS-PEKS(P，$pk_{FS}$，$pk_{BS}$，$wk_1$)，$T_{wk_2} \leftarrow$ DS-Trapdoor(P，$pk_{FS}$，$pk_{BS}$，$wk_2$)，则有

$$\text{BackTest}(P,\ sk_{BS},\ C_{ITS}) = \begin{cases} 0 & kw_1 = kw_2 \\ 1 & kw_1 \neq kw_2 \end{cases}$$

对于算法中安全参数 $\lambda$，在非对称密码算法中，其密钥都是通过 Setup 算法生成的，公钥加密的明文空间和签名的消息空间也是 Setup 算法事先确定的，为了衡量各个算法的复杂度，提出了安全参数 $\lambda$，用安全参数作为非对称密码算法的输入长度，通过安全参数，就可以度量方案的高效性和安全性. 对于系统参数 P，通过 Setup 算法，以安全参数 $\lambda$ 为输入，可以输出系统参数 P，用以生成服务器的公钥 / 密钥对.

### 2.2　线性同态平滑投影 hash 函数

构建用于关键字搜索的双服务器公钥加密的核心要素是平滑投影 hash 函数(Smooth Projective Hash Function，SPHF)，SPHF 是基于域 X 和 NP 语言 L 定义的，其中 $L \subset X$. 在语言 L 到集合 Y 上，由以下 5 种算法(SPHFSetup，HashKG，ProjKG，Hash，ProjHash)定义 SPHF 系统(表 1).

**表1 SPHF系统说明**

| 算法 | 输出 |
|---|---|
| SPHFSetup($1^\lambda$) | 全局参数 param，NP语言L的描述 |
| HashKG(L,param) | Hash秘钥 hk |
| ProjKG(hk,L,param) | 投影秘钥 hp |
| Hash(hk,L,param,W) | Hash值 hv$\in$Y |
| ProjHash(hk,L,param,W,w) | Hash值 hv′ |

其中，$W \in X\backslash L$ 表示语言，平滑投影 hash 函数满足正确性和平滑性，对于证据 w，正确性要求

$$\mathrm{Hash}(hk,L,param,W) = \mathrm{ProjHash}(hk,L,param,W,w) \tag{1}$$

对于任意 $W \in X\backslash L$，以下2个分布在统计上是不可区分的(图3).

$$V_1 = \{(L,param,W,hp,hv) \mid hv = \mathrm{Hash}(hk,L,param,W)\} \tag{2}$$

$$V_2 = \{(L,param,W,hp,hv) \mid hv \leftarrow Y\} \tag{3}$$

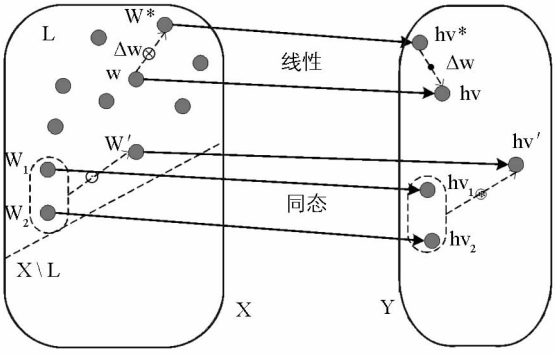


图3 线性同态SPHF

针对SPHF，提出一种线性同态SPHF，可以生成更安全的关键字搜索的双服务器公钥加密，如图3所示. 对于任何 $W \in L$，证据 w 和 $\Delta w \in W$，存在一个 $W^* \in L$，使得 $\Delta w \otimes W = W^*$. 对于任意的 $W_1$，$W_2 \in L$，$w_1$，$w_2 \in W$，存在一个 $W' \in L$，有 $W_1 \odot W_2 = W'$. 对于图3中符号的定义为

1) ◎：$\forall W_1, W_2 \in L$，$W_1 ◎ W_2 \in L$

2) ⊛：$\forall y_1, y_2 \in Y$，$y_1 \circledast y_2 \in Y$

3) $\odot$，$\oplus$：$\forall w_1, w_2 \in W$，$w_1 \odot w_2 \in W$，$w_1 \oplus w_2 \in W$

4) $\otimes$：$\forall w \in W$，$\forall W \in L$，$w \otimes W \in L$

5) $\bullet$：$\forall w \in W$，$\forall y \in Y$，$w \bullet y \in Y$

线性同态SPHF要求底层语言也是线性和同态语言，如果语言L满足以下属性，则它是线性和同态的.

1) 对于任意 $W \in L$，$w \in W$，$\Delta w \in W$，则有

$$\mathrm{Hash}(hk, \Delta w \otimes W) = \Delta w \bullet \mathrm{Hash}(hk, W) \tag{4}$$

当 $\Delta w \otimes W = W^*$，则有

$$\mathrm{ProjHash}(hp, W^*, w^*) = \Delta w \bullet \mathrm{ProjHash}(hp, W, w) \tag{5}$$

其中 $w^* = \Delta w \odot w$.

2) 对于 $\forall W_1, W_2 \in L$，$\forall w_1, w_2 \in W$，有

$$\mathrm{Hash}(hk, W_1 ◎ W_2) = \mathrm{Hash}(hk, W_1) \circledast \mathrm{Hash}(hk, W_2) \tag{6}$$

当 $W_1 \circledast W_2 = W'$，有

$$\mathrm{ProjHash}(hp, W', w') = \mathrm{ProjHash}(hp, W_1, w_1) \circledast \mathrm{ProjHash}(hp, W_2, w_2) \tag{7}$$

其中 $w' = w_1 \oplus w_2$.

线性同态平滑投影 hash 函数能够构建用于关键字搜索的双服务器公钥加密，提高了搜索框架的安全性.

## 3　实验结果与分析

为了验证本文云存储系统的有效性，从 2 个方面进行实验验证，①对云存储系统的性能和可靠性进行实验验证，②对安全云存储中双服务器 PESKS 的计算效率进行实验验证.

表 2 给出了不同云存储特性的对比结果. 对比云系统文献[10]中有基于密钥策略属性加密云存储框架，文献[15]中有隐藏访问模式的云存储方案，文献[16]中有基于属性加密的云存储系统，文献[17]中有多服务器多关键字加密云存储.

**表 2　不同方案特性对比**

| 性　　能 | 本文 | 文献[10] | 文献[15] | 文献[16] | 文献[17] |
|---|---|---|---|---|---|
| 分层网络结构 | 是 | 否 | 否 | 否 | 否 |
| 多用户 | 是 | 否 | 是 | 否 | 是 |
| 支持多存储引擎切换 | 是 | 否 | 否 | 否 | 否 |
| 大文件并发 | 是 | 否 | 否 | 否 | 是 |
| 文件恢复 | 是 | 否 | 否 | 否 | 否 |
| 关键词搜索 | 是 | 否 | 否 | 否 | 是 |
| 多服务器 | 是 | 否 | 否 | 否 | 是 |
| 加密 | 是 | 是 | 是 | 是 | 是 |
| 对抗 KGA | 是 | 否 | 否 | 否 | 否 |

对抗 KGA 攻击表示的是对抗关键字猜测攻击(Keyword Guess Attack，KGA). 由表 2 可以看出，本文双服务器的 PEKS 框架云储存系统在性能上优于其他现有方案，因为本文系统采用了分层网络结构，有效减少了攻击；通过存储引擎动态策略使存储系统在不同的存储引擎之间自由切换；采用 Master / Workers 设计模式实现大数据的并发读写，负载均衡、队列缓冲和 First-move First-failure 策略保证多用户大文件的存储效率；通过恢复令牌使得文件实现上传，保证文件上传/下载效率. 另外，基于线性同态 SPHF 的双服务器 PEKS 搜索框架，线性同态 SPHF 生成关键字搜索的双服务器公钥加密，保证用户数据安全，并能够对抗 KGA 攻击. 图 4 给出了多用户条件下，不同方案的平均响应时间.

从图 4 中可以看出，随着并发请求数量增加，文件上传的平均响应时间线性增加，当并发请求数达到 800 以后，平均响应时间增加幅度变大. 不过本文云存储系统的平均响应时间比现有存储系统都要少，这是因为 Master / Workers 模式队列缓冲和 First-move First-failure 策略保证了多用户大文件的存储效率.

从图 5 中可以看出，在不同的并发请求数量下，上传/下载数据发生的错误数量，随着并发请求数的增加，上传的错误量随着增加，不过本文云存储系统在恢复令牌机制下，使得错误量降低，优于其他系统.

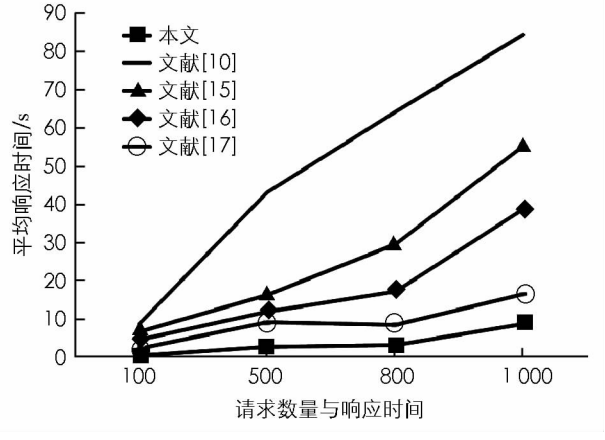


图 4　请求数量与平均响应时间关系图

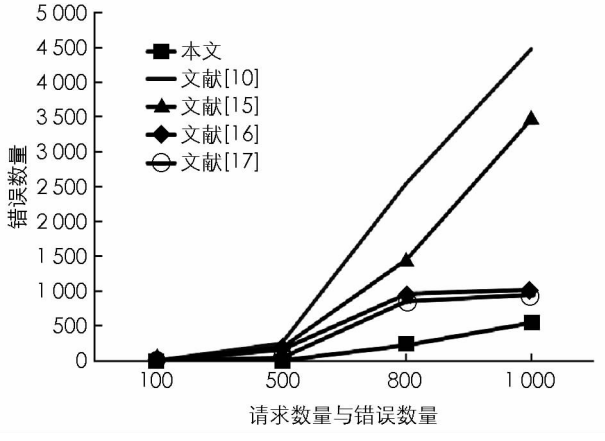


图 5　请求数量与错误数量关系图

作为商业存储服务，持久可用性非常重要. 为了分析云存储服务的持久可用性，引入了“可信度”概念，以表示服务在一定时间内保持正确的概率. 应用虚拟集群后，将通过负载平衡识别错误服务器，并且用户请求将自动切换到其他普通服务器，对于相同数量的用户请求，集群中的服务器数量越多，错误概率越低，

可靠性越高，但成本越高，因此可靠性和成本之间的权衡是云服务业务中的一个问题. $N$ 个平台服务器的可靠性如下所示.

$$R = 1 - \sum_{X=1}^{N} P(X) \tag{8}$$

其中，$P$ 是服从泊松分布的错误概率，$X$ 是错误的数量. 根据统计，当前集群中每千次平均请求错误数为0.03，可以得出本文系统的可靠性达到98.96%，满足设计需求.

对本文云存储系统中双服务器PEKS的计算性能进行实验，对比方法有文献[13]中无双线性对PEKS，文献[18]中指定服务器的可搜索公钥加密方案，文献[19]中抗关键词猜测攻击的可搜索公钥加密方案. 表3给出了性能对比结果，其中时间单位为ms，密文长度和陷门长度单位为bit.

**表3 本文方案与已有方法的对比结果**

| 指　　标 | 文献[13] | 文献[18] | 文献[19] | 本文 |
|---|---|---|---|---|
| 关键词加密时间 | 6.85 | 32.84 | 20.08 | 3.34 |
| 陷门产生时间 | 0.22 | 48.93 | 7.54 | 0.15 |
| 测试时间 | 2.21 | 78.06 | 57.12 | 1.15 |
| 密文长度 | 1 024 | 2 048 | 1 024 | 1 024 |
| 陷门长度 | 160 | 2 048 | 512 | 100 |

如表3所示，所有现有方案[13],[18],[19]都需要在生成PEKS密文和测试期间进行配对计算，因此效率低于本文的方案，因为本文方案不需要任何配对计算. 由表3可以看出，本文方法有最高的计算效率，适用于低通信带宽和计算受限的设备.

## 4 结　　语

本文设计一种多用户并发的分层云存储系统，提出了双服务器PEKS搜索框架，对网络分层，并引入存储引擎动态策略、First-move First-failure策略Master/Workers模式、恢复令牌和线性同态SPHF等算法，保证了大量用户的并发访问，使得文件上传和下载的错误率保持在可接受的范围内，提升了整个系统的存储效率和计算效率. 实验结果表明，多服务器集群将服务的可信度提高到98.96%，陷门产生的平均耗时仅为0.15 ms，相较于现有其他方案，对多用户具有较高的存储效率和计算效率，说明本文设计的云存储系统和搜索框架具有可行性和有效性.

**参考文献：**

[1] STERGIOU C, PSANNIS K E, KIM B, et al. Secure Integration of IoT and Cloud Computing [J]. Future Generation Computer Systems, 2018, 78: 964-975.

[2] ZHONG H, ZHU W L, XU Y, et al. Multi-authority Attribute-based Encryption Access Control Scheme with Policy Hidden for Cloud Storage [J]. Soft Computing, 2018, 22(1): 243-251.

[3] 宋　衍，韩　臻，李建军，等. 支持安全共享的云存储系统研究 [J]. 通信学报，2017，38(A01)：88-96.

[4] 刘毅文，黄显宁，文坤辉，等. 基于Docker的轻量级云存储系统研究 [J]. 计算机技术与发展，2018，28(11)：159-162.

[5] CHEN L B, QIU M K, SONG J, et al. E2FS: an Elastic Storage System for Cloud Computing [J]. The Journal of Supercomputing, 2018, 74(3): 1045-1060.

[6] 李　超，花　磊，宋云奎. 面向云计算的分布式应用自动部署框架 [J]. 计算机技术与发展，2018，28(6)：12-16.

[7] 刘竹松，何　喆. 基于Merkle哈希树的云存储加密数据去重复研究 [J]. 计算机工程与应用，2018，54(5)：85-90，121.

[8] LI J G, YAO W, HAN J G, et al. User Collusion Avoidance CP-ABE with Efficient Attribute Revocation for Cloud Storage [J]. IEEE Systems Journal, 2018, 12(2): 1767-1777.

[9] REN Z, WANG L, WANG Q, et al. Dynamic Proofs of Retrievability for Coded Cloud Storage Systems [J]. IEEE Transactions on Services Computing, 2018, 11(4): 685-698.

[10] 任鑫垚，李　毅，黄金涛，等. 基于密钥策略属性加密云存储安全框架设计与实现 [J]. 通信技术，2017，50(2)：340-345.

[11] 王少泫. 基于封闭环境的云存储安全方法研究 [D]. 保定：河北大学，2017.
[12] ZHAO W，QIANG L，ZOU H，et al. Privacy-Preserving and Unforgeable Searchable Encrypted Audit Logs for Cloud Storage [C]//2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). Shanghai：IEEE，2018.
[13] 徐海琳，陆　阳. 高效无双线性对的带关键词搜索的基于证书加密方案 [J]. 计算机应用，2018，38(2)：379-385.
[14] SUZUKI T，EMURA K，OHIGASHI T. A Generic Construction of Integrated Secure-Channel Free PEKS and PKE and Its Application to EMRs in Cloud Storage [J]. Journal of Medical Systems，2019，43(5)：1-15.
[15] 李宇溪，周福才，徐紫枫. 隐藏访问模式的高效安全云存储方案 [J]. 东北大学学报(自然科学版)，2018，39(8)：1086-1091.
[16] CHI P W，LEI C L. Audit-Free Cloud Storage via Deniable Attribute-Based Encryption [J]. IEEE Transactions on Cloud Computing，2018，6(2)：414-427.
[17] 黄海平，杜建澎，戴　华，等. 一种基于云存储的多服务器多关键词可搜索加密方案 [J]. 电子与信息学报，2017，39(2)：389-396.
[18] ISLAM S H，OBAIDAT M S，RAJEEV V，et al. Design of a Certificateless Designated Server Based Searchable Public Key Encryption Scheme [C]//International Conference on Mathematics and Computing. Singapore：Springer，2017.
[19] 徐海琳，陆　阳. 抗关键词猜测攻击的可搜索公钥加密方案 [J]. 计算机工程与应用，2018，54(24)：108-115.

# Efficient Cloud Storage System Based on Dual Server PEKS Framework

HUANG Feng-liang[1]，　QIAN Xiao-jie[2]

*1. Practice Teaching Center，Zhengzhou Railway Vocational & Technical College，Zhengzhou 451460 China；*
*2. School of Information Engineering，Zhengzhou University，Zhengzhou 450001，China*

**Abstract**：In order to reduce the cost of cloud storage users and to improve the efficiency of secure cloud storage，a multi-user concurrent cloud storage system has been designed，and a public key encryption with keyword search (PEKS) search framework based on dual server is proposed. The cloud storage system has been designed to freely switch between multiple storage method through the storage engine dynamic policy. It uses hardware load balancing，intermediate buffering and First-move First-failure strategy to deal with a large number of user access，improving request response rate and system stability. Parallel Master / Workers mode effectively handles a single large file request，and through the token mechanism for file transfer recovery and concurrent transmission. The proposed dual server PEKS search framework design a linear homomorphism smooth projection hash function，which makes the proposed search framework have higher security and solves the security vulnerabilities of traditional PEKS. The experimental results show that the proposed scheme can prevent internal keyword guessing attacks，and its average response time and computational efficiency are better than other existing schemes.

**Key words**：multi-user concurrency；keyword search；dual server；smooth projection hash function；cloud storage system

**责任编辑**　夏　娟