

RS 纠删码在云存储中的应用

余林琛, 章 巍, 林 强, 许杰星, 钟 贝

(中国地质大学 计算机学院, 湖北 武汉 430074)

摘 要: 云存储作为一种旨在为用户提供高效、廉价、安全、可扩展、可定制的存储服务的存储模式, 已然成为存储服务的发展趋势。但是因为其云端存储节点的不可控性, 云存储在如何保障数据安全性的问题上面临着挑战。通过将 RS 纠删码引入云存储中, 采用分片聚合机制, 为云存储的数据安全性保障提供了一种新的解决方案。

关键词: RS 纠删码; 云存储; 数据安全; 缓冲区

中图分类号: TP338.6

文献标识码: A

文章编号: 1000-7180(2011)08-0234-03

The Application of RS Erasure Codes in the Cloud Storage

YU Lin-chen, ZHANG Wei, LIN Qiang, XU Jie-xing, ZHONG Bei

(College of Computer, China University of Geosciences(Wuhan), Wuhan 430074, China)

Abstract: Cloud storage as a storage mode which designed to provide users with cheap, efficient, secure, scalable, customizable storage services, have become the trend of storage services. But because of its cloud storage node is not controllable, how to protect data stored in the cloud security issues facing challenges. RS erasure codes by the introduction of cloud storage, by fragmentation polymerization mechanism for cloud storage data security protection provides a new solution.

Key words: cloud storage; data security; RS erasure; buffer;

1 引言

在当今风起“云”涌的时代, 云存储作为“云”的基础架构和最广泛的应用得到了极大的重视。在云存储系统中, 用户数据存放于系统的云端, 而构成云端的存储节点是用户不可控的。用户的数据可能未经授权第三方挖掘比对或恶意篡改, 同时, 在云端单个或多个存储节点缺失、失效的情况下(随着云端的扩展, 存储节点故障的几率将增加), 用户数据丢失的可能性极大。上述情况说明, 云存储的发展亟需一种能完全保证用户数据完整性、隐私性和可靠性的安全机制^[1]。基于此, 本文提出将 RS 纠删码^[2]引入云存储中, 采用基于 RS 纠删码的数据分片方法, 把用户数据分成若干分片分别存储到不同存储节点。由于编码时将用户数据分段读入缓冲区, 因此分片数据不连续, 分片内容上的分散保证了数据私

密性, 并且由于纠删码的性质, 数据还原过程中对单个分片的依赖性低, 单个分片的缺失不会影响到数据的还原, 提高了数据的冗余能力^[3]。

2 RS 纠删码介绍

一个 (n, k) 纠删码将一个数据文件以字节为单位分为 k 个等长的数据块(不足的以 0 补齐), 通过编码生成 $m(m = n - k)$ 个上述长度的校验块, 在还原数据时, 只需要 n 个分块中的任意 k 个就可以恢复原文件。每个分块包含若干字节, 每个字节的长度为 w 位, $w \in \{8, 16, 32, 64\}$, w 可在程序设计时自由选择, 通常选择 $w = 8$, 因为系统中包含少于 256 个磁盘, 而且 $w = 8$ 表现最好。原数据表示为 $D_0, D_1, D_2, \dots, D_{n-1}$, 编码数据表示为 $C_0, C_1, C_2, \dots, C_{m-1}$, 每一个 D_i 或 C_j 都有 w 位, 即 $d_{i,0}, d_{i,1}, \dots, d_{i,w-1}$ 或 $c_{j,0}, c_{j,1}, \dots, c_{j,w-1}$, 则纠删码编码过程可表示为图 1:

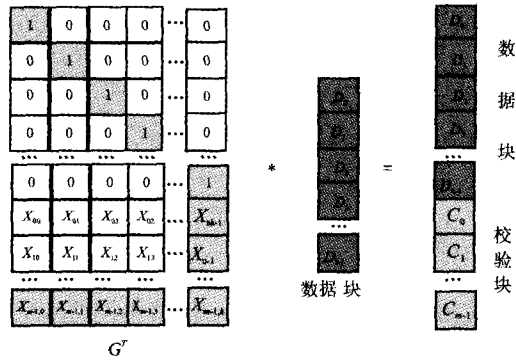


图1 纠错码编码过程

其中 $G_{m \times (m+k)}$ 由 m 阶范德蒙德(Vandermonde)矩阵通过线性变换得到,是数据还原的关键。

$$\text{构造形如} \begin{Bmatrix} a_1^0 & a_2^0 & \cdots & a_k^0 \\ a_1^1 & a_2^1 & \cdots & a_k^1 \\ a_1^2 & a_2^2 & \cdots & a_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_k^{n-1} \end{Bmatrix}$$

的 Vandermonde 矩阵,其中 $n = k + m$, k 为数据块的数量, m 为生成的校验块数量. 经过多次的线性行变换得到生成矩阵 G^T , 记为 G , 将现有数据 D 与 G 相乘后得到 E , 可表示为 $GD = E$:

$$G = \begin{Bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ x_{11} & x_{12} & \cdots & x_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mk} \end{Bmatrix}, \quad D = \begin{Bmatrix} d_1 \\ d_2 \\ \vdots \\ d_k \end{Bmatrix}, \quad E = \begin{Bmatrix} D \\ G \end{Bmatrix} \begin{Bmatrix} d_1 \\ d_2 \\ \vdots \\ d_k \end{Bmatrix}$$

生成矩阵 G 中 I 是一个 $k \times k$ 阶单位矩阵, P 是 $m \times k$ 阶校验产生矩阵. 产生矩阵 G 是由 Vandermonde 矩阵通过线性变换而来, 因此 G 中任意 m 行所组成的方阵都可以是可逆矩阵, 这个重要的性质是数据恢复过程必须要依赖的条件之一。

若有 m 个数据分块丢失, 删去 m 个数据分块在矩阵 G , E 中对应的行, 得到新的 $k \times k$ 阶矩阵 G' 和新的 $1 \times k$ 阶矩阵 E' , 显然有等式:

$$G'D = E'$$

恢复数据 D 时对上述等式进行计算, 即求 G' 逆矩阵. 因为由 G 中任意 k 行数据所组成的新矩阵 G' 都是可逆的, 即可以求得其逆矩阵 $(G')^{-1}$, 因此得

到以下等式:

$$(G')^{-1}G'D = (G')^{-1}E',$$

$$\text{即 } D = (G')^{-1}E'.$$

可以看出, 丢失的数据分块不超过 m 块时, 不会影响原数据文件的恢复。

3 RS 纠错码在云存储中的应用及优化

3.1 RS 纠错码在云存储中的应用

在应用于云存储时, 首先将用户文件分成 $X+1$ 个大小相等且为 k 的倍数的数据段(不足的用 0 补齐), 然后对每一个数据段作纠错码编码, 在存放编码后得到的数据块 D_i 与校验块 C_j 时, 按下标分别存放到不同的文件分片中, 例如文件数据段 0 的数据块 D_0 存放在分片 0 中, D_1 存放在分片 1 中, 数据段 1 的数据块 D_0 存放在分片 0 中, D_1 存放在分片 1 中, 依次类推^[4]. 文件分片流程图 2 所示。

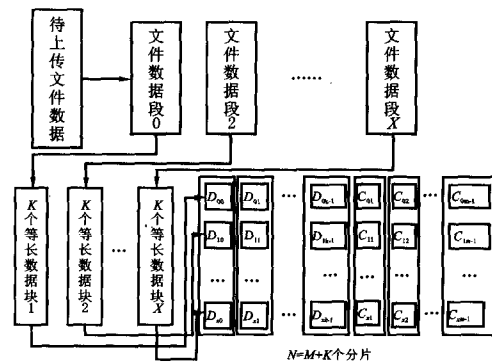


图2 文件分片流程图

通过分片机制得到的文件分片每一个都是由文件不同部分的数据块和校验块组成的, 分片中文件信息是分散的, 即单个文件分片不会泄漏用户数据信息, 这就保证了即使包括存储节点提供商在内的第三方非法取得单个节点上存储的分片, 也无法获得用户文件内容, 云存储中数据的隐私性得到可靠保障。

同时, 由范德蒙德矩阵性质可知, 在 $n = k + m$ 个分片中, 只要有 k 个分片能够正常使用, 系统就能完全恢复用户的原始文件. 这就意味着, 即使某些分片被恶意删改, 或者是系统中单个或多个存储节点失效时, 用户数据也不会丢失. 这一特点提高了云存储系统的容错性和冗余性, 为数据的可靠性和完整性提供了保障。

此外, 应用 RS 纠错码在恢复用户文件时, 最少只需要连接 k 个下载节点. 连接的下载节点越少下载速度越快, 下载延时越短. 应用该算法的优点在于出现网络丢包或错误时, 下载节点不需要采用重传

机制,只需要重新选择其他节点完成下载任务.

3.2 RS 纠删码在云存储中的优化

在对文件进行编码的过程中由于用户待上传文件的大小是不一定的,在上传的文件过大的情况下,需要读入内存的数据过多将导致编码效率的下降.因此,设置缓冲区分段读入文件数据是有必要的.然而如何在文件大小不断变化的情况下合理设置缓冲区大小,使得算法在编码任何大小的文件时都能保持最高效率,是缓冲区设置算法需要解决的问题.

在设计缓冲区自适应算法时,首先对两个不同大小的文件进行多组测试,测试结果如图 3 所示.

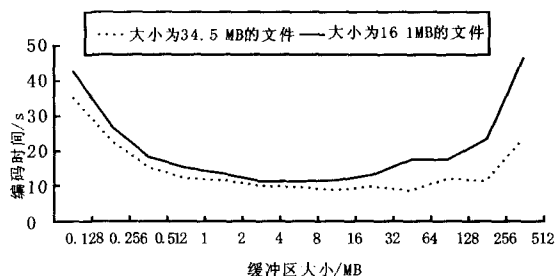


图 3 不同缓冲区大小设置下编码时间对比

易见在缓冲区大小为 2~16 MB 的时候,编码效率最高,因此设置缓冲区初值为 2 MB. 纠删码在编码过程中,涉及到的参数有文件读写单位 W 和文件分片数量 k ,同时要求每个进行计算的数据分片的大小能够被上述两个参数的乘积整除,因此缓冲区的设置需要考虑到这点.综上所述,缓冲区自适应算法的描述如下:

输入: k 值和 w 值;

输出: 缓冲区大小 buffersize 值;

步骤 1: 初始化 buffersize, 设值其初值为 2MB;

步骤 2: 如果 buffersize 不能被 $w * k$ 整除, 设置两个信号变量 up 和 down, 初值大小与 buffersize 相等; 步骤 3: 信号变量 up 和 down 同时分别自增和自减, 当其中一个能被 $w * k$ 整除时, 停止当前操作, 设置 buffersize 为该值.

应用该算法后, n 个分片中数据内容不是连续的, 而是来自不同的数据段, 这使得在数据恢复时缓冲区大小(buffersize)的值是必须获得的. 这就使得在无法获得编码缓冲区大小算法时, 数据恢复无法进行, 在一定程度上也保证了用户数据的私密性.

4 结束语

本文将 RS 纠删码引入云存储中, 在客户端采用基于 RS 纠删码的分片聚合机制对文件进行编码处理, 弱化了云端存储节点的不可靠性对数据安全性的影响, 保证了用户数据的隐私性、可靠性和完整性. 同时这种方法也存在着不足, 算法中没有对云端存储节点信息进行及时的检查和更新, 一旦大量存储节点信息丢失或遭篡改, 用户数据将无法恢复.

参考文献:

- [1] Hafner J L. WEAVER codes: highly fault tolerant erasure codes for storage systems[C]// Proceedings of the 4th Usenix Conference on File and Storage Technologies (FAST'05), San Francisco, CA: IEEE, 2005.
- [2] 张焕国, 刘玉珍. 密码学引论[M]. 武汉: 武汉大学出版社, 2004.
- [3] Bowers K D, Juels A, Oprea A. HAIL: A high-availability and integrity layer for cloud storage[C]// Proceedings of the 16th ACM conference on Computer and communications security (CCS'09), New York, NY: IEEE, 2009.
- [4] Wang C, Wang Q, Ren K, et al. Ensuring data storage security in cloud computing[C]// Proceeding of the 17th International Workshop on (IWQoS), Charleston, sc: IEEE, 2009: 1-9.

作者简介:

余林琛 女, (1977-), 讲师. 研究方向为网络安全、对等计算.

(上接第 233 页)

exploration of association rules with rule-focusing methodology[J]. KAIS, 13(1): 43 - 75.

- [5] Liu B, Hsu W, Wang K, et al. Aided exploration of interesting association rules[C]// proceedings of the 3rd Pacific-Asia Conference on Methodologies for knowledge Discovery and Data Mining. London, UK: springer-verlay, 1999.
- [6] Claudia Marinica, Fabrice Guillet. Knowledge-based

interactive postmining of association rules using ontologies [J]. IEEE Transactions on Knowledge and Data Engineering, 2010: 784-797,

作者简介:

张亚鹏 男, (1970-), 硕士研究生, 副教授. 研究方向为数据库、数据挖掘.

刘燕 女, (1963-), 硕士研究生, 教授. 研究方向为数据挖掘, 智能教学软件.