文章编号:1671-4598(2017)08-0279-04 DOI:10.16526/j.cnki.11—4762/tp.2017.08.072 中图分类号:TP391 文献标识码:A

一类高效的数据库系统安全存储策略研究

张生福
(青海民族大学 计算机学院,西宁 810007)

摘要:针对云存储环境下多副本方案存储效率低下的问题,设计了一种高效的数据安全存储策略;该策略采用了并行思想,设计了高效的数据同步存储算法;该算法将用户的存储请求同时转发给多个工作者,由这多个工作者同时向每个副本服务器写入数据;该策略将云端设计为整体协调、并行处理模式,即多个工作者由管理者统一分配调度,各个工作者独立地服务于对应的副本存储服务器,由管理者与用户进行交互处理,并且这多个工作者对用户来说是透明的,该设计模式并没有增加用户使用云存储的复杂度;实验结果表明,提出的数据安全存储策略在保证副本冗余的情况下可以有效地降低额外的时间损耗,保证用户读写云端数据的效率不低于单副本情况下的效率;该方案用于云存储环境下高效的数据安全存储是可行的、有效的。

关键词:云存储;多副本;数据安全;并行处理;数据库

Research on the Strategy of Efficient Data Safety Storage in the Cloud Storage Environment

Zhang Shengfu
(School of computer science, National University of Qinghai, Qinghai 810007, China)

Abstract: To solve the problem of the low efficiency of Multi-duplicate under the environment of Cloud Storage, this paper proposed a high-efficiency strategy of data safety storage. The strategy adopts the parallel processing ideology and designed the high-efficiency algorithm of the data parallel storage. The algorithm designed to transponder the request coming from the user to many workers, which write user data to the given duplicate server. The strategy is designed as the integrity coordination and the parallel processing mode, which is to say that all the workers are handled by the manager, and every worker is served to the given duplicate server. The manager handles the mutual actions with the users, and all the workers are transparent to the users. Thus the design mode does not increase the complexity for users to use the cloud storage. The experimental data indicates that the strategy this paper designed can decrease the time spoilage under the condition of Multi-duplicate and can ensure that the efficient of the read and write to the cloud not lower than the single-duplicate. The scheme is used for cloud storage environment and efficient data storage is feasible and effective.

Keywords: cloud storage; multi-duplicate; data safety; parallel processing

0 引言

云存储作为云计算的基础架构,在学术界和商界受到了高度的重视,无论是在学术界还是商业界,云存储正在被广泛的研究与应用[1-2]。云存储最重要的一点就是要保证数据的安全性,其中数据的容灾与恢复一直扮演着重要的角色[3-4]。在现实应用中,磁盘损坏、机房断电、地震火山等自然灾害、机房网络故障,都有可能发生[5-6]。云存储应该接受这种现实并且允许这些情况的发生,并且在这些情况发生时,还能不间断地继续对外提供数据服务[7-8],因此一个高效的数据安全存储策略是十分必要的。

面对磁盘损坏,需要将数据存储多个副本;机房停电,可以给机房配备备用电源;地震火山等自然灾害导致机房被毁,需要将数据存储在远隔千里的免于数据被毁的一个地方,机房网络故障,有些可以恢复,但有些无法恢复,此时,只能依靠远在千里的备用机房[9-10]。数据的多副本备份无疑是解决这个问题的关键,但是,多副本存储需要大量的额外的存储时间,这对用户来说,体验是不好的[11]。目前,数据的多副本存储是主要的保证数据安全的方式,但是在目前的研究中,多副本的实现是以额外的时间消耗为代价的[12],这种情况下,用户对数据的上传、下载等操作需要花费更多的时间,这对用户来说,无疑是一个不好的体验。

为了解决多副本存储额外的时间消耗问题,本文设计了一个高效的数据安全存储策略,在该策略设计过程中,充分地利用了并行执行的高效性设计了数据同步算法,该算法不仅能够保证数据冗余,而且能够及时地响应用户请求。

1 高效数据安全存储策略的设计

本文设计的数据安全存储策略中充分地利用了并行执行的高效性设计了数据同步算法,该算法不仅能够保证数据冗余,而且能够及时地响应用户请求,即该算法能够保证不损失用户的请求与响应时间。

1.1 总体设计方案

本文设计的高效的数据安全存储策略模型中,客户端请求与某一个数据中心的管理服务器建立连接后,管理服务器会将与客户端的请求转接到相关的所有副本服务器、以及对等数据中心的所有副本服务器,将数据并行存储到所有的副本服务器中。在该策略的设计过程中,考虑到对用户时间的响应效率,只要同一个数据中心的副本有三分之二正确返回,就认为数据

收稿日期:2017-05-04; **修回日期**:2017-05-22。
基金项目:国家民委高等教育教学改革研究项目(15072)。
作者简介:张生福(1965-),男,青海西宁人,硕士,副教授,主要从事数据库系统设计以及 ERP 设计方向的研究。

已经被正确保存到云端，此时，就给客户端返回正确的存储结果。由于转接是无时间损耗的，三分之二的结果返回也能在一定程度上节省存储时间，因为存储速度快的服务器先返回，在网络环境中，由于网络传输的不确定性，这种方案无疑提高了相对平均存储速度。

云存储环境下的高效数据安全存储策略的整体方案如图 1 所示。在该存储策略中，设计了两个数据中心，但是，并在实际应用中，可以设计更多的数据中心，以保证数据更加安全可靠。在每个数据中心都有若干副本，副本数目至少保证在三个以上。在每个数据中心都有一个管理服务器，它不但负责与客户端的通信，并且还负责与对等的数据中心通信，完成用户的数据请求响应与不同数据中心的数据相互备份。同时，管理服务器还承担着分发用户请求的职责，将用户请求并发地转发到对应的所有副本存储服务器。

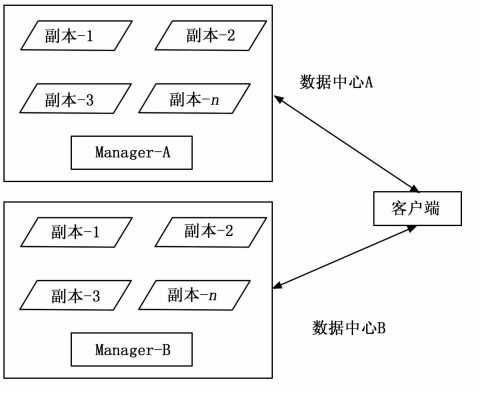

图 1　数据安全存储策略设计图

这种存储策略不但可以让用户更加高效的完成数据请求，而且，数据在云端的存储也更加高效与安全。如果将数据中心部署在不同的地域范围，还可以达到自然灾害情况下的容灾。使得数据的安全系数大大提高。

本文将就客户端的几种数据请求流程设计作详细介绍，主要包括写入数据到云端、从云端读取数据、删除云端数据等。以下的流程设计图都是在图 1 的存储策略设计图的基础上进行的，即有两个数据中心。对于多于两个数据中心的流程，完全可以从只有两个数据中心的流程中进行扩展。

1.2　写入数据流程设计

客户端写入数据到云端的流程设计如图 2 所示。客户端在需要上传数据到云端时，首先会与数据中心的管理服务器 Manager－A 建立连接，如果与 Manager－A 建立连接失败，则会与数据中心的管理服务器 Manager－B 建立连接，如果与 Manager－B 建立连接失败，则返回给客户端失败信息。如果建立连接成功，则由 Manager 负责转发与客户端的数据请求，将请求并发传送到所有的副本中。

数据写入流程步骤设计如下：

1）客户端尝试着与数据中心的管理服务器建立连接，如果与 Manager－A 建立连接失败，则尝试与 Manager－B 建立连接，只要有一个成功即可；如果都失败了，则返回给客户端建立连接失败的结果；

2）与客户端成功建立连接的管理服务器 Manager 则负责与客户端的数据传送；

3）Manager 根据副本数目以及对等数据中心的数量，创建数目相等的工作者，每个工作者负责一个副本的写入工作；

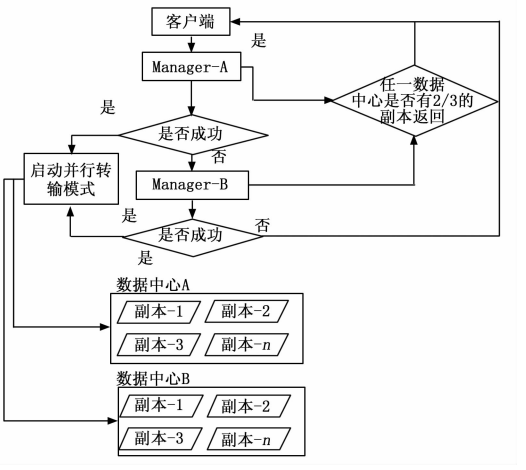

图 2　写入数据流程设计

4）如果写入副本的工作者有三分之二都返回成功，则返回给客户端写入成功的结果；

5）直至客户端将所有的数据写入云端；Manager 结束与客户端的连接；

Manager 新建的工作者对客户端都是透明的，客户端无法感知这些连接的存在。这些工作者并发工作，同时进行副本写入工作，相互之间并没有任何影响，所以，它们的存在对客户端写入数据到云端并没有任何的时间损耗，相反，由于网络的不稳定性，网络并无法保证单一的传输路线快速的传输，在本设计中，只要多个路线有三分之二返回，就将存储结果返回给客户端，那么在整体上来说，加速了客户端的数据传输效率。

1.3　读取数据流程设计

客户端云端读取数据的流程设计如图 3 所示。客户端在需要从云端读取数据时，首先会与数据中心的管理服务器 Manager－A 建立连接，如果与 Manager－A 建立连接失败，则会与数据中心的管理服务器 Manager－B 建立连接，如果与 Manager－B 建立连接失败，则返回给客户端失败信息。如果建立连接成功，则由 Manager 负责从所有的副本中找到一个正确的最新的副本，由该副本所在的服务器响应客户端的请求。

从云端读取数据的步骤设计如下：

1）客户端尝试着与数据中心的管理服务器建立连接，如果与 Manager－A 建立连接失败，则尝试与 Manager－B 建立连接，只要有一个成功即可；如果都失败了，则返回给客户端建立连接失败的结果；

2）与客户端成功建立连接的管理服务器 Manager 则负责查找到一个最新的正确的副本；

3）该副本所在的服务器负责与客户端进行通信，完成数据传输；

从数据读取的流程可以看出，Manager 选择的副本服务器直接与客户端进行数据传输工作，这就可以在客户端请求较多的情况下大大减轻每个副本服务器上的压力，使得每个副本服务器都可以高效率的工作。

1.4　删除数据流程设计

客户端删除云端数据的流程设计如图 4 和如图 5 所示。本

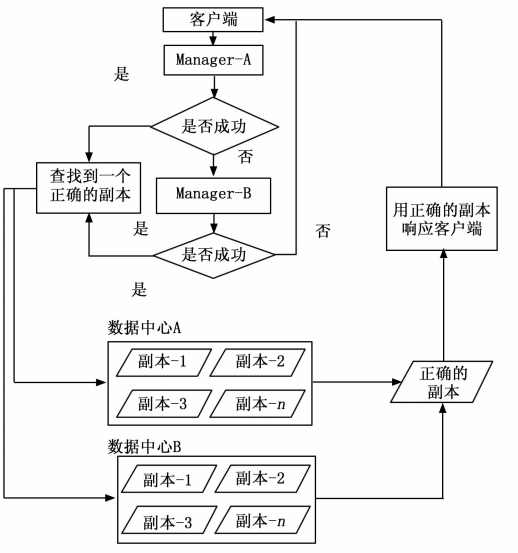

图 3　读取数据流程设计

设计将数据删除划分为了逻辑删除与物理删除两个步骤。采用逻辑删除主要是为了提高用户请求的响应速度，并且，减轻云端存储服务器的负担。逻辑删除发生在用户请求删除数据的时候，而物理删除是后台进程周期性进行的。后台进程周期性扫描管理节点，将标记为删除的记录对应的数据从系统中删除。

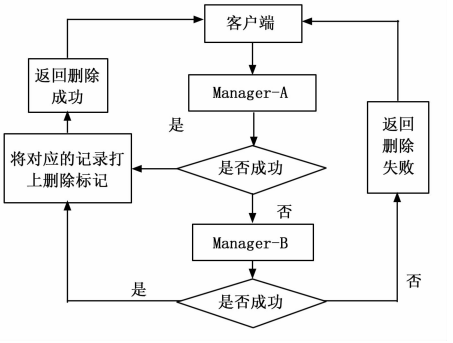

图 4　逻辑删除数据流程设计

数据逻辑删除流程步骤设计如下：

1）客户端尝试着与数据中心的管理服务器建立连接，如果与 Manager－A 建立连接失败，则尝试与 Manager－B 建立连接，只要有一个成功即可；如果都失败了，则返回给客户端建立连接失败的结果；

2）与客户端成功建立连接的管理服务器 Manager 负责将本数据中心的记录相关数据的元数据记录标记为已删除；

3）返回给客户端处理结果；

图 4 展示的是逻辑删除流程，也是客户端可以感知到的流程，该流程仅仅将对应的记录标记为已删除，并不会讲用户请求的删除数据从云端真正的删除。真正的物理删除由图 5 所示的流程完成。

数据的物理删除步骤设计如下：

1）周期性的触发删除流程；

2）由数据中心 A 的管理服务器 Manager－A 执行删除流程；

3）Manager－A 查找已经被标记为已删除的记录；

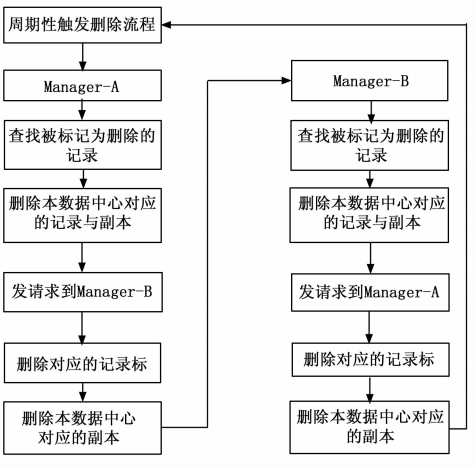

图 5　数据物理删除流程设计

4）将记录对应的数据副本从云端系统删除，并删除该记录；

5）发送请求到 Manager－B，删除该记录在数据中心－B 中的记录以及所有副本；

6）直至数据中心 A 中被标记为已删除的所有记录都得到处理；

7）由数据中心 B 的管理服务器 Manager－B 执行删除流程；

8）Manager－B 查找已经被标记为已删除的记录；

9）将记录对应的数据副本从云端系统删除，并删除该记录；

10）发送请求到 Manager－A，删除该记录在数据中心－B 中的记录以及所有副本；

11）直至数据中心 B 中被标记为已删除的所有记录都得到处理；

12）至此，一个周期性的物理删除操作结束。

该流程设计每执行一次，在该期间被逻辑删除的所有数据都会被清理干净，这种设计方式可以集中删除无用数据，将这种操作放在服务器比较清闲的时间段执行，会大大的减轻服务器负担，提高服务器响应客户端的效率，也可以提高服务器资源的利用率。

1.5　数据副本恢复方案设计

在数据的某一个副本失效或者数据中心无法提供服务时，需要为数据重建新的副本以保证副本的最低限度，并且，当数据中心恢复正常时，也要保证能够把在这段时间内数据的变化同步到恢复正常的数据中心。

数据副本恢复与数据中心数据恢复的流程设计如图 6 所示。其大致思想就是遍历管理节点的所有数据记录，如果有数据记录的副本数目不够规定的数目，则为其新建副本，直到所有的数据副本都能达到预定的数目；然后检测之前是否有数据中心不可达，如果有，则当数据中心恢复心跳时，就将该段时间内的变化数据同步到故障的数据中心，使得各个数据中心的数据达到一致。

副本的重建设计：检测程序周期性的检测所有文件的副本，如果发现数据副本有无法到达的，就需要为该副本重新找到新的服务器，从能够使用的副本服务器将数据复制到新的副

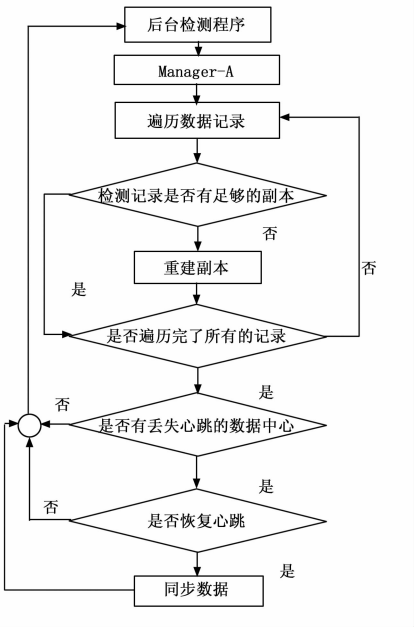

图 6 数据恢复方案流程图设计

本服务器，从而保证最小的副本数量，使得数据达到预定的安全程度。

数据中心的重建设计：数据中心都有检测程序，检测对等数据中心的心跳，如果发现对等数据中心的心跳丢失，就会记录当前的时刻，等待对等数据中心恢复心跳时，将这期间发生的所有数据变更都要同步过去，以保证所有的数据中心数据的同步性。

副本和数据中心的重建都是由后台程序执行的，并不会中断数据中心对用户的服务。重建工作使得云端数据更加安全可靠，使云存储可以更好地服务于用户。

2 实验与分析

为了验证本文设计的高效数据安全存储策略，本实验设置了若干对照组，在不同的情况下分别统计上传、下载、删除用户数据的时间以及当前的副本个数。

2.1 实验设计

2.1.1 实验环境

为了简化实验环境，但尽可能模拟真实的应用环境，本文在两个不同的网段内分别部署了 5 台 PC 机。每个网段相当于一个数据中心，五台 PC 机中，有一台用来部署 MySQL 数据库，扮演 Manager 角色，用来保存用户的元数据；其他四台 PC 机用来保存数据副本，每台 PC 机保存一份副本。本实验限制用户数据的副本个数为 3，即数据副本个数总数为 3，不能大于这个限制。之所以部署四台 PC 机来存储用户数据，是为了验证本文设计的策略中，数据恢复部分的可行性与正确性。各 PC 机分配情况与组网的情况如表 1 所示。

2.1.2 实验步骤

1）在客户端放置 4 个 1G 的音频文件 file－1，file－2，file－3，file－4；

2）在所有的设备都运行正常的情况下，上传 file－1 到云端，记录上传消耗的时间，记录在表 2 中；

3）查询各数据中心 file－1 的副本数，记录在表 2 中；

表 1 PC 机分配与组网情况

数据中心	设备	功能
数据中心－1	PC－1	Manager
	PC－2	副本存储
	PC－3	
	PC－4	
	PC－5	
数据中心－2	PC－6	Manager
	PC－7	副本存储
	PC－8	
	PC－9	
	PC－10	

4）从云端读取 file－1，记录读取 file－1 的时间，记录在表 2 中；

5）删除 file－1，记录删除时间，再次执行步骤 3）；

6）关闭 PC－1 和 PC－6 的网络，模拟 PC－1 和 PC－6 故障；

7）对 file－2 重复执行类似于步骤 2）～步骤 5）的操作；

8）关闭 PC－2 和 PC－7 的网络，模拟 PC－2 和 PC－7 故障；

9）对 file－3 重复执行类似于步骤 2）～步骤 5）的操作；

10）关闭 PC－3 和 PC－8 的网络，模拟 PC－3 和 PC－8 故障；

11）对 file－4 重复执行类似于步骤 2）～步骤 5）的操作；

12）恢复所有 PC 的网络

13）上传 file－1 到云端，查询 file－1 在各数据中心的副本数和所在的 PC，记录在表 3 中（第一行）；

14）关闭数据中心－1 中的一个副本所在 PC 的网络，2 min 后，查询 file－1 在各数据中心的副本数和所在的 PC，记录在表 3 中（第二行）；

15）关闭数据中心－2 的网络，模拟数据中心故障；

16）上传 file－3 到云端，查询 file－3 在各数据中心的副本数和所在的 PC，记录在表 3 中（第三行）；

17）恢复数据中心－2 的网络，一段时间后，查询 file－3 在各数据中心的副本数和所在的 PC，记录在表 3 中（第四行）；

2.2 实验结果与分析

通过搭建实验环境，并按照上述实验步骤执行实验，得到的实验结果如表 2 和表 3 所示，其中，表 2 记录了在不同副本数情况下，上传、下载、删除数据所消耗的时间；表 3 记录了副本服务器故障以及数据中心故障时，副本的自动恢复能力。

表 2 不同副本数情况下数据操作时间 s

副本服务器数	上传	下载	删除
4	22	25	1
3	24	26	1
2	25	27	1
1	23	28	1

由表 2 的实验数据可以看出，副本数目的增多并没有使得数据的上传、下载、删除等操作消耗多余的时间。随着副本数

（下转第 303 页）

务为依据区分逻辑关系分别确定，这样将装备置于任务中进行评估更具科学性；理想解首选装备研制或出厂的理论数据更具“理想”性，同时克服了以最优“样本”为理想解的样本本身带来的误差。装备评估结果中引入“合格分数线”使评估结果等级不再是一个无量化依据的模糊量，使评估结果的可信度更高。

本文方法简单易懂，评估过程紧贴装备所担负目标任务等实际情况，评估不受装备评估指标样本大小影响，结果较准确可靠，既适合单一装备的可靠性评估也适用于多台装备的可靠性评估。

参考文献：

[1] 郭忠来，吴　华，胡永刚，等. 基于数据深度的设备状态评估模型研究 [J]. 系统工程与电子技术，2014，36 (5)：897－899.

[2] 宋　飞. 多机协同条件下机载雷达的效能评估研究 [D]. 郑州：郑州大学，2015：28－39.

[3] 严英杰，盛　戈，王　辉，等. 基于高维随机矩阵大数据分析模型的输变电设备关键性能评估方法 [J]. 中国电机工程学报，2016，36 (2)：435－445.

[4] 马庆跃. 武器装备体系作战效能综合评估技术研究 [J]. 哈尔滨工业大学，2015：7－20.

[5] 何　迪，章　禹，郭创新. 一种面向风险评估的输电线路故障概率模型 [J]. 电力系统保护与控制，2017，45 (7)：69－75.

[6] 王义冬，刘　义，石伟峰. 基于作战效能的武器装备可靠性指标评估方法 [J]. 现代防御技术，2011，39 (5)：166－170.

[7] 贾治宇. 武器装备通用特性指标体系研究 [A]. 大型飞机关键技术高层论坛及中国航空学会 2007 年学术年会论文集 [C]. 2007：1－5.

[8] 胡元潮，阮江军，杜志叶. 基于 TOPSIS 法的变电站一次设备智能化评估 [J]. 电力自动化设备，2012，32 (12)：22－27.

[9] 党兴华，李全升. 基于熵权改进 TOPSIS 的陕西国家级高新区创新发展能力评价 [J]. 科技管理研究，2017，3：75－83.

(上接第 282 页)

目的增多，数据读写效率并没有降低，即是说，本文设计的高效存储策略并没有随着副本数目的增多而增加额外的耗时。

表 3　数据故障恢复情况记录表

	数据中心－1		数据中心－2	
	副本数	所在的 PC	副本数	所在的 PC
步骤 13	3	1、2、3	3	6、7、8
步骤 14	3	1、2、4	3	6、7、8
步骤 16	3	1、2、4	0	无
步骤 17	3	1、2、4	3	6、7、8

由表 3 的实验数据可以看出，如果某一个副本服务器无法继续提供服务时，管理者服务器会将坏掉的服务器上的数据副本重新在其他服务器上重建，努力保证数据副本的个数；当数据中心无法提供服务期间，数据无法保存到该数据中心，但是，当该数据中心恢复提供服务时，其他数据中心就会将在此期间的数据变化在该数据中心重建。

实验结果表明，本文设计的高效的数据安全存储策略是可行的、有效的。该策略在不增加额外的时间损耗的情况下，可以保证数据的多副本存储、副本的重建与数据中心的数据重建。这种机制可以最大限度的保证数据安全。

3　结语

云计算的快速发展使云存储的数据安全变得越来越重要。但是保证数据安全的多副本策略会大大降低数据上传、下载等操作的效率，使得用户浪费大量的宝贵时间。为了解决多副本问题对时间的过渡消耗问题，提高用户上传、下载数据的效率，本文设计了一个高度并行的数据安全存储策略。该策略采取了多线程多数据连接，每个线程负责一个数据连接的方式，使得用户数据可以同时和多个副本服务器进行交互，大大提高了用户数据的存储效率，并且由于是多副本，也保证了数据的安全性。下一步的研究计划是实现数据下载时副本的选择策略，使得用户可以选择一个速度更快的副本来实现下载功能。

参考文献：

[1] 傅颖勋，罗圣美，舒继武. 安全云存储系统与关键技术综述 [J]. 计算机科学，2013，50 (1)：136－145.

[2] Wang C，Chow S S M，Wang Q，et al. Privacy－preserving public auditing for secure cloud storage [J]. IEEE Transactions on Computers，2013，62 (2)：362－375.

[3] 李　晖，孙文海，李凤华，等. 公共云存储服务数据安全及隐私保护技术综述 [J]. 计算机应用研究，2014，51 (7)：1397－1409.

[4] Iacono L L，Torkian D. A System－Oriented Approach to Full－Text Search on Encrypted Cloud Storage [A]. 2013 International Conference on Cloud and Service Computing (CSC) [C]. IEEE，2013：24－29.

[5] 付艳艳，张　敏，陈开渠，等. 面向云存储的多副本文件完整性验证方案 [J]. 计算机应用，2014，51 (7)：1410－1416.

[6] Yang K，Jia X. An efficient and secure dynamic auditing protocol for data storage in cloud computing [J]. Parallel and Distributed Systems，IEEE Transactions on，2013，24 (9)：1717－1726.

[7] Terry D B，Prabhakaran V，Kotla R，et al. Consistency－based service level agreements for cloud storage [A]. Proceedings of the Twenty－Fourth ACM Symposium on Operating Systems Principles [C]. ACM，2013：309－324.

[8] 乔宏明，姚文胜. 基于策略提升公共云存储信息安全水平的方案研究 [J]. 计算机工程与设计，2013，37 (21)：53－57.

[9] Yang K，Jia X，Ren K，et al. Dac－macs：Effective data access control for multi－authority cloud storage systems [A]. INFOCOM，2013 Proceedings IEEE [C]. IEEE，2013：2895－2903.

[10] 杨继慧，周奇年，张振浩. 基于物联网环境的云存储及安全技术研究 [J]. 计算机应用与软件，2013，18 (6)：12－16.

[11] Qian W，Wen Q，Jin Z，et al. An Architecture of Secure Searchable Cloud Store [A]. Proceedings of the 2013 Fifth International Conference on Multimedia Information Networking and Security [C]. IEEE Computer Society，2013：596－599.

[12] Chen L. Using algebraic signatures to check data possession in cloud storage [J]. Future Generation Computer Systems，2013，29 (7)：1709－1715.