计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
49(Suppl.): 19-25, 2012

云存储服务中可证明数据持有及恢复技术研究

陈兰香　　许　力
(福建师范大学数学与计算机科学学院　福州　350108)
(福建师范大学网络安全与密码技术重点实验室　福州　350108)
(lxiangchen@fjnu.edu.cn)

Research on Provable Data Possession and Recovery Technology in Cloud Storage

Chen Lanxiang and Xu Li
(*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou* 350108)
(*Key Laboratory of Network Security and Cryptology, Fuzhou* 350108)

Abstract　Cloud storage achieves the goals that users can access their data anywhere and at any time. It can also comply with a growing number of legislations. For users whose storage requirements are unpredictable and users who need low-cost storage, the cloud storage is a good choice for its convenience and efficiency. Moreover, cloud storage saves investment at the same time it also saves social resources and energy. However, because of security, reliability and service levels, cloud storage has not yet been widely recognized and utilized. When users store their data in the cloud storage, they most concern about whether the data is complete and correct; if there is a failure, whether it can be recovered. So, let users verify that the storage server keeps on holding their data completely and correctly is significant. This paper reviews the state of the art research works on provable data possession and recovery technology. Then the application of these technologies in cloud storage considering its special requirements is discussed. It points out the directions of provable data possession and recovery technology in cloud storage.

Key words　cloud storage; storage security; reliability; provable data possession; data recovery

摘　要　云存储可以实现任意地点、任意时间、任意数据访问及保障法规遵从的需求等.对存储需求不可预测、需要廉价存储的用户来说,按需购买存储容量的云存储与一次性购买整套存储系统相比显然会带来更多的方便和效益,且云存储在为用户节省投资的同时也节约了社会资源与能源.但是,因为云存储的安全性、可靠性及服务水平等还存在众多问题亟待解决,所以云存储还未得到人们的广泛认可与使用.当用户将数据存放在云存储中,他们最关心的是数据是否完整无误;如果出现故障,是否可以恢复其数据.所以,在云存储中只有让用户可以验证存储服务提供者正确地持有其数据,且当检测到错误时可实现数据恢复,他们才可放心地使用云存储.综述了可证明数据持有及恢复技术在国内外的研究现状,讨论了云存储服务的安全性与可靠性需求,并研究云存储服务对可证明数据持有及恢复方案的特殊要求,从而明确在云存储环境下可证明数据持有及恢复技术的研究方向.

关键词　云存储;存储安全;可靠性;数据持有性验证;数据恢复

中图法分类号　TP302.7

收稿日期:2012-01-04

基金项目:福建省自然科学基金项目(2011J05148);福建省高校产学合作科技重大项目(2010H6007);福建省教育厅科技项目(JA10079, JB10041)

图灵奖获得者吉姆·格雷(Jim Gray)在其获奖演说[1]中指出:由于互联网的发展,未来每18个月新产生的数据量将是有史以来数据量之和.人类社会产生的数据信息一方面来自于互联网,一方面来自于日常生产及各种科学试验,例如科学计算和仿真、飞行动力学、核爆炸仿真、太空探测及医疗影像数据等每天所产生的数据信息更是大到了惊人的程度[2].

信息存储系统朝无限的带宽、无限的容量和无限的处理能力(infinite bandwidth, infinite capacity, infinite processing capability),即"3i"方向发展,提出"Anytime, Anywhere, Anything"的目标,即要求数据在任意时间、任意地点实现任意数据访问.存储产品不再是附属于服务器的辅助设备,而成为互联网中最主要的花费所在.信息技术正从以计算为核心的计算时代进入到以存储为核心的存储时代,网络化存储将成为未来存储市场的热点.而目前的云存储服务是网络存储发展的必然趋势.

首先介绍云存储服务的意义与重要性,然后介绍国内外目前在可证明数据持有和恢复技术方面的研究现状,在第四部分讨论了云存储服务的安全性与可靠性需求,并研究云存储服务对可证明数据持有及恢复方案的特殊要求,最后进行总结.

1 云存储服务

目前对云存储(cloud storage)的定义众说纷纭,但是云存储的特点可概括为:1)存储容量和性能的高可扩展性;2)地理位置的无约束性;3)随需付费模式.

高德纳(Gartner)咨询公司预测到2012年,20%的公司将不再拥有自己的IT资产而转向云.在日立数据系统公司公布的《2010年十大存储投资方向》报告[3]中,云存储位列第二.存储市场具有无限的潜力,而云存储是信息存储的趋势,它可为用户带来如下好处:1)无需购置初始耗资较大的服务器,也免去了专业的服务器及数据管理人员,避免过大的投资;2)实现任意地点、任意时间、任意数据访问;3)提供可用性、可维护性与扩展性保障;4)保障法规遵从的需求;5)实现数据长期保存.

云存储的主要特色是容量规模大,使用多少,支付多少,上不封顶,下不设限.有了云存储,永远也不会出现存储空间不足的情况.对存储需求不可预测、需要廉价存储阵列或低成本长期存档的用户来说,按需购买存储容量的云存储与一次性购买整套存储系统相比显然会带来更多的方便和效益.并且,云存储在为用户节省初始投资的同时也节约了社会资源与能源.

云存储具有众多优点,但是因为用户对云存储服务的安全性、可靠性及可用性等问题有所怀疑,所以目前还没有得到人们的广泛认可与使用.特别地,在微软弄丢了Sidekick用户的数据,SwissDisk的文件管理器出现崩溃故障,Amazon S3宕机频繁,曾经一次持续了8 h,哪个用户还敢将数据托付给云存储服务呢?即便是著名品牌服务商也没有担保其云存储服务的安全性与可靠性.

引用美国前总统罗纳德·里根的一句名言,"要我相信你,请你先证明给我看(trust but verify)".所以在云存储中,让用户可以验证服务提供者正确地持有其数据,且如果检测发生错误时可以恢复其数据是一件很有意义的研究工作.

如果用户都信任云存储服务提供者,或者是服务提供者确实做到了安全可靠地存储用户的数据,那么云存储将具有无限的潜力,它在为用户带来方便和效益的同时,也为社会节约了大量的资源与能源.

2 可证明数据持有与恢复技术

可证明数据持有和恢复技术是验证不可信的存储服务器是否正确地持有(保存)数据,避免存储服务提供者删除、篡改数据,并确保存储数据的可恢复性.目前的研究工作主要集中在可证明数据持有(provable data possession, PDP)方案和可恢复证明(proof of retrievability, POR)方案.PDP和POR方案的主要区别是:PDP方案可检测到存储数据是否完整,但无法确保数据可恢复性;POR方案保证了存储数据的可恢复性.通常,考核数据持有性证明方案优劣的指标有:

(a) 数据访问量,方案需要访问的数据量;

(b) 计算开销,指用户预处理文件、服务器生成证据及用户验证的计算开销;

(c) 通信开销,用户与服务器间的数据传输量;

(d) 存储开销,指需要的额外的存储空间;

(e) 允许的更新操作,包括数据修改、插入、添加、删除;

(f) 验证次数,允许验证的次数;

(g) 是否支持公开验证;

(h) 检测概率,能够检测到错误的概率;

(i) 可恢复性,出错时是否可以恢复数据;

(j) 安全性证明方案,包括标准模型下的安全性证明和随机预言模型下的安全性证明.

下面将根据评价指标综述 PDP 方案和 POR 方案及其相关工作在国内外的研究现状.

2.1 PDP 方案

文献[4]最早提出远程数据的完整性检查,使用基于 RSA 的 Hash 函数对整个文件计算 Hash 值.其原理为:令 N 为 RSA 模数,F 为代表文件的大整数,$g\in \mathbf{Z}_N^*$,检查者保存 $a=g^F \bmod N$;在挑战中,检查者生成任意元素 r 并发送 g^r 到服务器,服务器返回 $s=(g^r)^F \bmod N$,检查者计算 a^r,并验证等式 $s=a^r \bmod N$ 是否成立.因为该方法基于公钥密码技术,所以方案的计算开销很大.文献[5]的原理与此相同,但其目的是阻止数据传输中的欺骗.

约翰·霍普金斯大学(Johns Hopkins University)的 Ateniese 等人在这方面做了一些研究工作,他们在文献[6]中第 1 次正式定义 PDP 方案,文中提出的 2 个 PDP 方案都是使用同态可验证标签(homomorphic verifiable tags),用户为每个数据块生成一个 Tag,将此 Tag 连同数据存放在服务器上.验证时,用户随机选择一些块向服务器发出挑战,要求服务器返回持有这些块的证据.服务器利用请求块及相应的标签生成持有证据,因为同态性,多个文件块的标签可以聚合成一个值,因此极大地节省了响应带宽.用户通过验证响应信息确认数据拥有,而不需要检索数据.提出的方案只需要用户维护常量的元数据信息,服务器的开销也近似为一个常量,挑战应答只要 1 Kb 左右,实验表明方案的性能受限于磁盘 I/O 而不是密码计算.文中作者第 1 次提出公开验证的方法.但是该方案在生成证据时使用基于 RSA 的模指运算,也没有考虑数据更新问题.并且该方案的多个服务器可以共谋(collusion attacks),所以不适用于多复本协议.

他们在文献[7]中提出在随机预言模型(random oracle model)下使用任何具有同态属性的鉴定协议(identification protocol)构造公钥同态线性认证器(homomorphic linear authenticator, HLA)的通用机制,并表明怎样将任何公钥 HLA 转化为公开可验证的存储证明方案(proofs of storage, PoS),使通信复杂度与文件长度无关,并且支持无限次验证.但是该方案也是基于公钥密码技术.在文献[8]中,他们提出基于对称密码技术构造 PDP 方案.该方案在初始化时,由用户设定要挑战的次数和内容,将响应作为元数据存放在用户端,因此,更新次数和挑战次数都是有限的.而且只支持 append-类型的插入,也不支持公开验证.同时,他们所在的研究小组第 1 次提出多复本 PDP (multiple-replica PDP, MR-PDP)方案[9],允许用户通过挑战应答协议验证服务器存储文件 t 个复本:1)每个复本是可用的;2)使用 t 倍的存储空间存储数据的 t 个复本.MR-PDP 扩展了文献[6]的单拷贝的情况,还可以增加新的复本,而不需要对文件进行预处理.该方案首先将数据加密,然后将加密数据与 t 个不同的随机掩码异或.该方案仍然基于 RSA,也没有考虑数据更新问题.

清华大学的舒继武教授等人提出的数据持有性检查(data possession checking, DPC)[10]是国内第 1 篇关于数据持有性证明的论文.方案的基本思想是在一次挑战中,检查者指定文件中 c 个随机位置的数据块和一个密钥 k_2,服务器根据这些数据块和密钥 k_2 由单向 Hash 函数 $h(\cdot)$ 计算出一个 Hash 值,并和一个与之对应的校验块一起返回给检查者,检查者检查 Hash 值和校验块是否匹配以确定应答是否有效.同时提出一个基于校验块循环队列的挑战更新机制,允许动态增加检查者可发起的有效挑战的次数.分析表明检查者端的存储开销和检查者和服务器间的通信开销均为常数量级.测试结果表明一次置信度为 99.4%的持有性检查的计算开销为 1.8 ms,和磁盘 I/O 开销相比可以忽略不计.方案通过避免使用公钥密码系统,将文件预处理的计算开销降低了 3 个数量级.

布朗大学(Brown University)的 Erway 等人提出 2 种动态数据持有性证明方案(dynamic PDP, DPDP)[11]实现数据更新.一种使用基于等级的鉴别跳表(rank-based authenticated skip lists),一种基于 RSA 树结构.他们的主要工作是实现动态性,即实现插入操作.整个方案仍然是基于 RSA 的模指运算.

文献[12]利用基于 RSA 的 Hash 函数的同态性,可以在初始化时间开销与用户的存储开销间进行权衡,该方案也是基于 RSA,用户和存储服务器都有模指运算.文献[13]提出利用同态 Hash 构建同态标签实现无限次数据持有性验证.文献[14]提出利用代数签名实现数据持有性验证,该方案简单高效,其基本方案只支持有限次数据验证,作者提出一种挑战更新方案.文献[15]提出一种高效的数据持有性证明,作者还提出一种基于 RSA 的挑战更新机制,但它们的缺点仍然在于没有考虑数据的动态性.

2.2 POR 方案

RSA 实验室的 Juels 和 EMC 公司的 Kaliski 第 1 次提出 POR 的概念[16]，并提出基于“哨兵”(sentinel)的 POR 方案. 其基本思想是首先将文件加密并使用纠错码编码，在编码后的文件中随机插入和文件数据不可区分的“哨兵”；检查者在挑战时要求服务器返回在这些随机位置的“哨兵”. 他们证明只要服务器以大于一定值的概率作出有效应答，则文件是可恢复的. 因为每挑战一次就消耗一个岗哨，并且没有挑战更新机制，因此只能进行有限次的挑战. 因为编码及增加的“哨兵”导致文件的膨胀率达到 15%.

加州大学圣地亚哥分校的 Shacham 和德克萨斯大学奥斯汀分校的 Waters 在文献[17]中提出的 2 个方案也是使用同态标签：一个方案基于伪随机函数，不支持公开验证；另一个方案基于 BLS 签名[18]，支持公开验证. 他们使用纠删码编码，但是没有考虑数据更新问题. 在文献[19]中，Dodis 等人第 1 次提出 POR 码，并对其进行形式化及理论分析工作，给出了几个将 POR 码转换为 POR 方案的方法. 他们提出在安全性与其他参数(如使用次数、挑战位置和服务器存储开销等)之间进行权衡的方案，但文中没有特别考虑通信开销及计算开销，也没有考虑数据更新问题.

RSA 实验室的 Bowers 等人在文献[20]中提出一个设计 POR 的理论框架，用于改进已有方案的 POR 构造，实现更低的存储开销和更高的检错率. 他们指出关于文件更新及公开验证仍然是未解决的公开问题. 他们在文献[21]中提出的 HAIL 方案在多个存储服务提供者之间作数据副本或冗余，然后使用 POR 方案检测数据是否被破坏. 当检测到某一服务提供者的数据被破坏时，可以利用其他服务器的数据进行恢复. 作者提出将 MAC 码嵌入奇偶校验块中. 首先 HAIL 使用分散码(dispersal code)将文件块分散到不同服务器上，因为 MAC 和奇偶校验块都可以基于 UHFs (universal hash functions)，因此就可能创建一个块同时是 MAC 和奇偶校验块. 基于这个思想，作者构造保护完整性的纠错码 IP-ECC，结合 PRFs, ECCs 及 UHFs，实现纠错码的同时也是一种抵抗破坏的 MAC 码. 文中对攻击模型有一个重要的约束条件：在一个给定的时间段，只能控制 n 个服务器中的 b 个，这样的一个时间段叫作 epoch，那么过了 n/b 个 epoch，数据可能都被破坏. HAIL 方案保护静态数据的完整性，不能进行数据更新，也不能进行公开验证.

Curtmola 等人集成前向纠错码(forward error correcting codes, FEC)到 PDP 方案中[22]，他们考虑不同的 FEC 编码有不同的性能、灵活性、纠错码效率和数据输出格式等. 他们认为 RS 编码效率太低，所以将原始文件交换位置，从中选择一部分进行 RS 编码，从而提高编码效率；而且攻击者不知道冗余码是从哪些块计算得到的，可以提高安全性.

2.3 其他方案

圣塔克莱拉大学(Santa Clara University)的 Schwarz 和加州大学圣克鲁兹分校(UCSC)的 Miller 在文献[23]中提出使用线性纠删码将数据编码，使用代数签名(algebraic signature)对块计算指纹. 因为代数签名具有同态属性，而且 ECC 是线性码，所以只要在相同的域上计算签名和奇偶校验，就可以使用数据的签名计算得到唯一的奇偶校验的代数签名. 他们考虑的是 P2P 的环境下，将数据编码后分条存放在 Internet 上的普通机器上.

HP 实验室的 Shah 等人在文献[24]中提出了基于数据委托的方案. 基于加密文件的 MAC，第三方审计者通过挑战应答验证存储服务提供者持有一个加密的文件. 因为挑战是预计算的，只能进行有限次的验证，元数据也随挑战次数线性增长；并且方案只能用于加密的文件，要求审计者维护长期的状态信息. 在文献[25]中他们提出了具有隐私保护特性的方案，即不向第三方泄露任何信息. 该方案也只能用于加密的文件，也要对整个文件计算 MAC 以及使用 MAC 验证数据持有性，有较大的计算和存储开销，且没有考虑数据更新问题及相关数据恢复技术.

布朗大学(Brown University)的 Heitzmann 等人在文献[26]中提出验证服务器响应的数据与用户执行的更新是否一致. 该方案不同于 PDP 方案，其目标不在于检测到数据破坏，而是验证服务器响应的数据与 Client 执行的更新一致，因此，响应数据只被用于验证完整性，并且只在请求文件的时候才执行. 方案使用鉴别跳表维护认证信息，支持简单快速的更新. 他们实现了一个在 Amazon S3 上的原型系统，用户只需存放一个 Hash 值，存储开销为 $O(1)$，服务器的计算开销是 $O(\log(n))$. Sebé 等人在文献[27]中提出的方案基于 Diffie-Hellman 问题，要求用户为每个块存放 N 位 RSA 模位数，因此其存储开销随块数线性增长，并且协议要求服务器访问整个文件.

新加坡国立大学的 Chang 和 Xu 在文献[28]中提出 Remote Integrity Check (RIC)，RIC 方案结合文

献[5]中基于 RSA 的方案和文献[29]中基于 ECC 的鉴定器,它不是 POR 系统,但是所有在 RIC 下证明安全的方案也可用于 POR 系统. RIC 的目标在于只需要验证者存放少量的额外信息就可以定期地检测远程服务是否保存了一个大文件. 但是他们的方案也继承了文献[5,29]中方案的缺陷,基于公钥密码技术,并且要求对整个文件取幂,计算开销很大. 在文献[30]中,Yamamoto 等人也提出使用基于 RSA 的同态 Hash 函数进行数据持有性验证,同时作者还提出使用批验证提高效率.

伊利诺理工大学(Illinois Institute of Technology)的 Wang 在文献[31]中第 1 次在云计算环境下考虑数据存储的安全性,他们提出的方案可以定位发生错误的服务器,并实现了部分数据更新操作,在接下来的工作[32]中,他们提出结合基于 BLS[18] 的同态鉴别器和 MHT,支持公开验证和数据更新. 在文献[33]中,他们考虑的是引入一个第三方的审计者,结合随机掩码技术实现隐私保护,不向第三方审计者泄露信息. 但是他们的数据持有性证明方案都是基于公钥密码技术,且没有考虑相关数据恢复技术.

2.4 方案比较

根据方案的评价指标,一些方案的对比见表 1,首先 PDP 方案一般不提供数据恢复技术,另外上述的各种方案或者基于公钥密码技术,所以计算开销很大,或者无数据更新方法,只能用于静态归档存储,或者挑战次数有限,不支持公开验证.

表 1 方案的各项指标比较

文献	(a)	(b) c/s	(c)	(d) c/s	(e)	(f)/(g)	(h)	(i)	(j)
[22]	$O(n)$	$O(1)/O(n)$	$O(n)$	$O(1)/O(n)$	N/A	∞/no	$1-(1-f)^c$	yes	N/A
[6]	$O(1)$	$O(1)/O(1)$	$O(1)$	$O(1)/O(n)$	a	∞/yes	$1-(1-f)^c$	N/A	RO
[8]	$O(1)$	$O(1)/O(1)$	$O(1)$	$O(1)/O(n)$	amd(t)	t/no	$1-(1-f)^c$	no	RO
[7]	$O(n)$	$O(n)/O(n)$	$O(1)$	$O(1)/O(n)$	N/A	∞/yes	$1-(1-f)^c$	N/A	ST
[11](DPDPII)	$O(n)$	$O(\log n)/O(n^{\varepsilon}\log n)$	$O(\log n)$	$O(1)/O(n)$	amid	∞/no	$1-(1-f)^{\Omega(\log n)}$	N/A	ST
[21]	$O(n)$	$O(\log n)/O(\log n)$	$O(1)$	$O(1)/O(n)$	N/A	∞/yes	$1-(1-f)^c$	yes	ma

说明:允许的更新操作为:append(a), modify(m), insert(i), delete(d),t 表示允许有限次数的操作. n 为文件的块数,f 为被破坏的块的比例,C 为请求验证的块数. ma 是 mobile adversary 简写,c 表示用户(client),s 表示服务器(server). ST 表示标准模型下的安全性,RO 表示随机预言模型下的安全性.

如果考虑数据可恢复性时,必然会增加用户和服务器的计算开销,那么为了公平,这里的计算开销只指发起挑战与响应的计算开销. 而且不同的可恢复方案,其冗余度与纠错能力也有不同. 总之,根据国内外研究现状可知,现有方案存在如下一些缺陷:1)基于公钥密码技术,所以计算开销很大,特别是数据量大的时候;2)没有考虑数据更新问题,因此只能用于静态归档存储;3)只能进行有限次数据持有性验证;4)不支持公开验证;5)没有考虑相关数据恢复技术,检测到破坏而不能恢复,因此实用性不强;6)有些方案没有安全性证明,因此不能确保其安全性;7)有些方案不适用于云存储服务环境;8)众多方案的效率有待进一步提高.

3 云存储服务对方案的需求研究

云存储服务是一种面向服务的网络存储,由用户与存储服务提供者组成. 用户将数据存放在服务提供者的服务器上,然后定期或不定期地验证其数据是否仍然完整无误. 一般来说,对于云存储服务提供者,他可能会:

1) 为了节约成本,丢弃不被访问或访问较少的数据,或将在线数据迁移到低速存储设备上;

2) 掩盖由于管理失误、硬件故障或者受到攻击而引起的数据丢失事件;

3) 篡改用户数据,或者泄漏用户数据;

4) 不能达到声称的性能、可靠性,比如声称存放了 t 份复本,而事实上只有 1 份拷贝.

因此,对于用户来说,云存储服务安全性和可靠性主要集中在如下几个方面:1)数据的机密性保障;2)数据的完整性保护;3)数据的可用性与可靠性保障. 数据的机密性可以通过加密实现,完整性通过对数据计算摘要. 但是,如何让用户确信其数据仍然正确无误地存放在云存储服务提供者的存储设备上,我们称之为存储服务的数据持有性验证,这是一个亟待攻克的研究课题. 此外,检测到数据受到破坏

[18] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. Journal Cryptology, 2004, 17(4): 297-319

[19] Dodis Y, Vadhan S, Wichs D. Proofs of retrievability via hardness amplification //LNCS 5444: Proc of TCC'09. Berlin: Springer, 2009: 109-127

[20] Bowers K D, Juels A, Oprea A. Proofs of retrievability: theory and implementation //Proc of CCSW'09. New York: ACM, 2009: 43-54

[21] Bowers K D, Juels A, Oprea A. HAIL: A high-availability and integrity layer for cloud storage //Proc of CCS'09. New York: ACM, 2009: 187-198

[22] Curtmola R, Khan O, Burns R. Robust remote data checking //Proc of StorageSS'08. New York: ACM, 2008: 63-68

[23] Schwarz T J E, Miller E L. Store, forget, and check: Using algebraic signatures to check remotely administered storage // Proc of ICDCS'06. Piscataway, NJ: IEEE, 2006: 1-12

[24] Shah M A, Baker M, Mogul J C, et al. Auditing to keep online storage services honest //Proc of HotOS'07. Piscataway, NJ: IEEE, 2007: 1-6

[25] Shah M A, Swaminathan R, Baker M. Privacy-preserving audit and extraction of digital contents. Cryptology ePrint Archive, 2008. [2011-11-02]. http://eprint.iacr.org/2008/186.pdf

[26] Heitzmann A, Palazzi B, Papamanthou, et al. Efficient integrity checking of untrusted network storage //Proc of StorageSS'08. New York: ACM, 2008: 43-54

[27] Sebé F, Balleste A M, Deswarte Y, et al. Time-bounded remote file integrity checking, 04429. Toulouse, France: Laboratary for Analysis and Architecture of Systems, 2004

[28] Chang E C, Xu J. Remote integrity check with dishonest storage server //LNCS 5283: Proc of ESORICS'08. Berlin: Springer, 2008: 223-237

[29] Naor M, Rothblum G N. The complexity of online memory checking //Proc of FOCS'05. Piscataway, NJ: IEEE, 2005: 573-584

[30] Yamamoto G, Oda S, Aoki K. Fast integrity for large data // Proc of SPEED'07. Amsterdam: IST, 2007: 21-32

[31] Wang C, Wang Q, Ren K, et al. Ensuring data storage security in cloud computing //Proc of IWQoS'09. Piscataway, NJ: IEEE, 2009: 1-9

[32] Wang Q, Wang C, Li J, et al. Enabling public verifiability and data dynamics for storage security in cloud computing // LNCS 5789: Proc of ESORICS'09. Berlin: Springer, 2009: 355-370

[33] Wang C, Wang Q, Ren K, et al. Privacy-preserving public auditing for data storage security in cloud computing //Proc of INFOCOM 2010. Piscataway, NJ: IEEE, 2010: 1-9

陈兰香 女,1979年生,博士,讲师,中国计算机学会会员,主要研究方向为计算机系统结构、网络存储、信息安全.

许 力 男,1970年生,教授,博士,中国计算机学会会员,主要研究方向为无线网络与移动计算、网络与信息安全.