一种基于雾计算思想的私密性云存储方案

周际援，罗皓，邱磊，王田
（华侨大学计算机科学与技术学院，福建 厦门 361021）

摘 要：云存储作为云计算服务的核心应用之一，凭借其庞大的云服务器存储容量吸引了大量用户。然而，在这种存储模式下，用户将数据完全存储在云服务器上从而失去对数据的控制权，存在很大的隐私泄露风险。传统的隐私保护方案通常建立在加密基础上，但这类方法无法有效防范来自服务器内部的攻击，若密码被泄露则数据随之被泄露。提出一种基于雾计算模式的三级安全云存储方案，通过设计的 Hash-Solomon 编码算法，将少量数据存储在雾服务器及本地，既可以充分利用云服务强大的存储空间，又可以保护数据不被泄露。通过安全性理论分析和实验测试证明了所提方案的可行性，是对现有云存储方案的有力补充。

关键词：云存储；雾计算；隐私保护；三级安全云存储
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2019.00087

Privacy cloud storage scheme based on fog computing

ZHOU Jiyuan, LUO Hao, QIU Lei, WANG Tian
Department of Computer Science and Technology, Huaqiao University, Xiamen 361021, China

Abstract: As one of the core applications in cloud computing field, cloud storage attracts a large number of users depending on its powerful storage capacity. However, in this storage schema, users' data is stored completely in cloud server. In other word, users' right of control on data is lost and users are facing privacy leakage risk. Traditional privacy protection scheme is usually based on encryption technology, but the attack from the inside of cloud server can't be resisted effectively by these kinds of methods. Once the password gets compromised, users' data will be stolen. In order to solve this problem, a three-level secure cloud storage scheme based on fog computing was proposed and a Hash-Solomon code algorithm was designed. A small part of data was stored in local machine and fog server, which can take full advantage of cloud storage and protect the privacy of data. Through the theoretical safety analysis and experimental test, the feasibility of our scheme is proved, and it is really a powerful supplement to existing cloud storage scheme.

Key words: cloud storage, fog computing, privacy protection, three-level secure cloud storage

1 引言

21 世纪以来，随着计算机技术的飞速发展，诞生了许多新技术。云计算技术自从在 2006 年的搜索引擎大会（SES San Jose 2006）上首次被提出并被 NIST（national institute of standards and technology）定义以来[1]，一直受到社会各界的关注。现阶段，云计算技术的发展已逐渐成熟，并派生出许多相关技术。

随着网络带宽和无线网络的快速发展[2]，用户数据量呈几何级增长，本地存储容量已经无法满足用户需求，将数据存储在公用的云服务器上成为未来存储的发展趋势[3]。如今国内外已有多家公司提供各具特点的云存储服务，如 Dropbox、Google

收稿日期：2018−07−27；**修回日期**：2019−02−21
基金项目：国家自然科学基金资助项目（No.61772148，No.61672441）；福建省自然科学基金资助项目（No.2018J01092）
Foundation Items: The National Natural Science Foundation of China (No.61772148, No.61672441), The Natural Science Foundation of Fujian Province of China (No.2018J01092)

Drive、iCloud、百度云盘以及有道云笔记等。

云存储服务存在着各种各样的问题，其中隐私问题尤为严重。历史上有多家云存储服务商曾发生过隐私泄露事件，如苹果公司的 iCloud 曾在 2014 年发生“泄露门”事件，众多好莱坞女星存储在云服务器上的私人照片遭窃取，使得其他普通用户担心存储在云服务器上的数据存在被泄露的风险。云存储服务的数据隐私问题主要是因为云存储系统中的用户没有实际控制数据的物理存储，造成了数据的所有权和管理权分离[4]。因而云服务提供商（CSP，cloud service provider）可以随意获取或搜索用户存储在云服务器上的数据，同时攻击者也可能通过攻击 CSP 的服务器获取用户数据，给用户带来了信息泄露或数据丢失的风险。传统安全云存储解决方案对于以上问题通常采用访问限制、数据加密等方法进行处理，但无论加密算法如何改进，都无法很好地解决来自云服务器内部的攻击。

本文提出了一种基于雾计算的三层安全云存储方案，结合 Reed-Solomon（RS）编码设计 Hash-Solomon（HS）编码[5-6]，将用户待存储的文件分割后分别存储在云服务器、雾服务器及本地中，利用编码性质保证其无法由部分数据还原。并使用 Hash 函数对各部分数据进行处理，保证了局部信息的隐私性。与现有的主流加密算法如 ABE（attribute-based encryption）、AES、DES 以及 RSA 等相比，所提方案的创新性包括如下 3 个方面。

1) 在传统云存储架构体系中引入雾计算模式，提出一种新的存储方案，以全新的思路考虑云存储中的安全问题。

2) 设计 HS 编码，通过合理编码以及巧妙的分配策略，保证数据安全性，解决了传统方法无法解决的内部攻击问题。

3) 通过仿真实验模拟，证明了方案的可行性。

2 相关工作

云存储系统安全在学术界和工业界一直备受关注，国内外关于安全云存储架构的研究有很多。

文献[7]针对云计算中的隐私保护问题，提出了支持隐私保护的云计算模型，并设计了一种支持隐私保护的加密方案 CESVMC（computable encryption scheme based on vector and matrix calculation），支持加密字符串的模糊检索和加密数值的加、减、乘、除 4 种算术运算，可以有效抵挡攻击者的破解，达到 IND-CCA 安全[8]，同时具有较好的加/解密性能。文献[9]针对传统云服务器加密提出了一种介于企业内网和公有云平台之间的私有云模型 TBS（Tsinghua bistu storage），其作用为在企业将原始数据上传至公有云之前，先经过企业私有管理平台对数据进行加密，再由该平台和公共云服务上传数据，从而保证数据不会以明文方式上传，解决了传输过程中的隐私泄露问题。文献[10]指出云存储的安全核心是分布式系统的安全性和私密性，在 SSL 和 Daoli 的基础上提出一种安全虚拟保护方案[11]，通过 SSL 协议传输数据，并在服务器端部署 Daoli，使得数据在传输过程中和写入硬盘前都被加密。文献[12]提出了一种高效的公共安全审计协议，用于全球数据块验证。通过该协议使得数据保护变得动态、高效。此外，在文献[13]中提出了一种基于云服务的都市数据共享架构，认为 CSP 是半可信的，因此采用基于属性的加密算法，保护用户数据不被可能存在的潜在攻击威胁。

上述研究针对云存储中的数据隐私保护进行改善，采用不同的加密策略，在数据存储、数据传输以及身份验证等不同阶段进行加密处理。然而在 CSP 不可信的情况下，上述研究提出的方案无法有效抵御来自服务器内部的攻击，也无法预防 CSP 由于某些目的利用用户数据牟取利益，因为用户数据完全存储在云服务器上，一旦被恶意用户获取，那么数据会面临被破解的危险。因此，本文提出了一种全新的安全云存储策略，通过将文件进行特殊分割处理，并且结合三层存储结构，实现用户数据的高度安全性。

3 基于雾计算思想的安全云存储系统

云存储的安全性是衡量云存储系统的重要标准，其中，数据安全性是云存储安全性的关键。数据安全性包含 3 个部分：数据私密性、数据完整性和数据可用性[14]。保证隐私和数据的完整性是相关领域研究的重点[15]，其中数据私密性是用户最关心的部分，也是本文研究的重点。本章将详细介绍本文提出的一种基于雾计算思想的三级安全云存储方案。

3.1 雾计算结构

雾计算是云计算的延伸，由思科（Cisco）的 Bonomi[16]于 2011 年首次提出，认为和云计算类似，雾计算也十分形象，大自然中的雾相比于云更贴近地面，因此用雾描述介于云和传感器网络之间的计算模型。雾计算相比于高度集中的云计

算，更接近边缘网络，地理分布更广泛，具有高实时性和低时延，对于一些对时延敏感的应用来说，雾计算更合适[17]。相比于传感器节点，雾计算节点具有一定的存储能力和数据处理能力，能够简单处理一些数据，进行简单应用，尤其是基于地理位置的应用。

雾计算结构通常是三层结构。最上层为云计算层，具有强大的计算和存储能力；第二层是由雾节点组成的雾节点层，作为雾计算结构的中间层，具有承接云计算层和传感器网络层的重要作用。其中，雾节点具有一定的计算和存储能力，可以将本地化、实时性要求高的应用放在雾节点层处理。底层为传感器网络层，主要作用是收集数据[18]，并将数据上传到雾节点层，雾节点层和其他层之间的传输效率高于云服务器和底层直接传输[19]。

3.2　基于雾计算思想的三级安全云存储架构

本文提出一种基于雾计算思想的三级结构安全云存储架构，以保护用户数据隐私[20]。云存储中内部攻击难以防范，传统方案如数据加密算法在面对外部攻击时效果显著，但当 CSP 内部出现问题时，该类方案无法解决[21]。本文所提出的三级安全云存储方案所面临的主要挑战首先是内部攻击，由于传统方法无法解决来自 CSP 内部的攻击，因此方案首先要解决这一问题，为了保护用户数据的安全隐私，采用编码方式将用户文件分为大、中、小 3 个部分。其中，每部分都缺失一定的关键数据，再结合雾计算模式，将这 3 个部分数据按从大到小的顺序分别存储在云服务器、雾服务器和本地中。通过此方法，攻击者即使得到某层服务器所有的数据，也无法还原用户的原始数据。

基于雾计算思想的三级安全云存储架构如图 1 所示，充分利用雾服务器的存储和数据处理能力，对用户准备存储在云服务器的文件进行编码。分割出约 1%的数据存储在本地，剩余 99%的数据上传至雾服务器，雾服务器再对文件进行编码分割，将约 4%的数据存储在雾服务器中，剩余数据全部传至云服务器存储，上述两次分割操作基于 HS 编码进行。HS 编码是本文设计的一种基于 RS 编码的数据编码方式，使用该编码对数据进行编码后，数据被分为 k 份并生成 m 份冗余数据。根据 HS 编码的性质，在 $k+m$ 份数据中，若拥有至少 k 份数据则可以还原完整的原始数据，若少于 k 份数据则无法还原完整的原始数据。本研究的思想基于 HS 编码特性，每次编码后将不多于 $k-1$ 份数据存储在存储性能较高的存储服务器上，剩余数据存储在低层存储服务器上。通过此方法，即使部分数据遭到窃取，窃取者也无法还原原始数据，从而保证了用户数据的私密性。

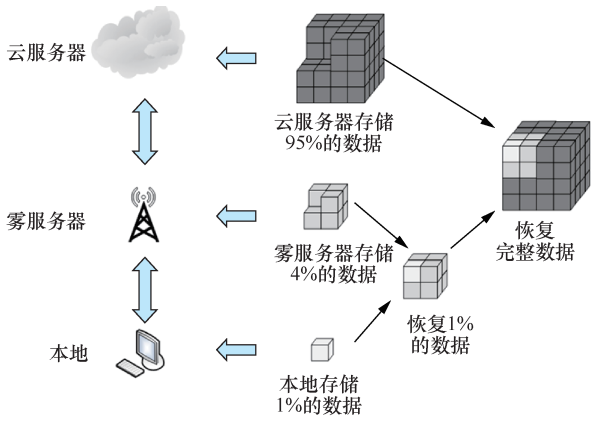

图 1　基于雾计算思想的三级安全云存储架构

3.3　方案具体实现细节

当用户需要将某个文件存储到云服务器时，用户存储文件流程如图 2 所示。

1) 在本地将文件进行 HS 编码并分为若干数据块，保存生成的编码信息（编码时产生的矩阵及 Hash 编码信息）以及部分数据块（本地存储数据块数量由实际情况决定），剩余数据块上传至雾服务器。

2) 雾服务器收到来自用户本地发送的数据块后，在雾服务器上再次对收到的数据块进行 HS 编码，将其分割为更小的数据块，选出部分数据块及编码信息存储在雾服务器上，剩余数据块上传至云服务器。

3) 云服务器收到雾服务器发来的数据块后，通过云存储管理系统进行分配，将数据块分别存储在不同服务器上，并记录这些服务器的关联信息。

当用户需要从云服务器读取文件时，用户读取文件流程如图 3 所示。

1) 当云服务器收到用户请求后，通过云存储管理系统，将分布存储的数据块整合并返回给雾服务器。

2) 雾服务器收到来自云服务器的数据后，根据存储在本地的 HS 编码信息，结合雾服务器的数据，还原部分数据，再将此部分数据返回给用户。

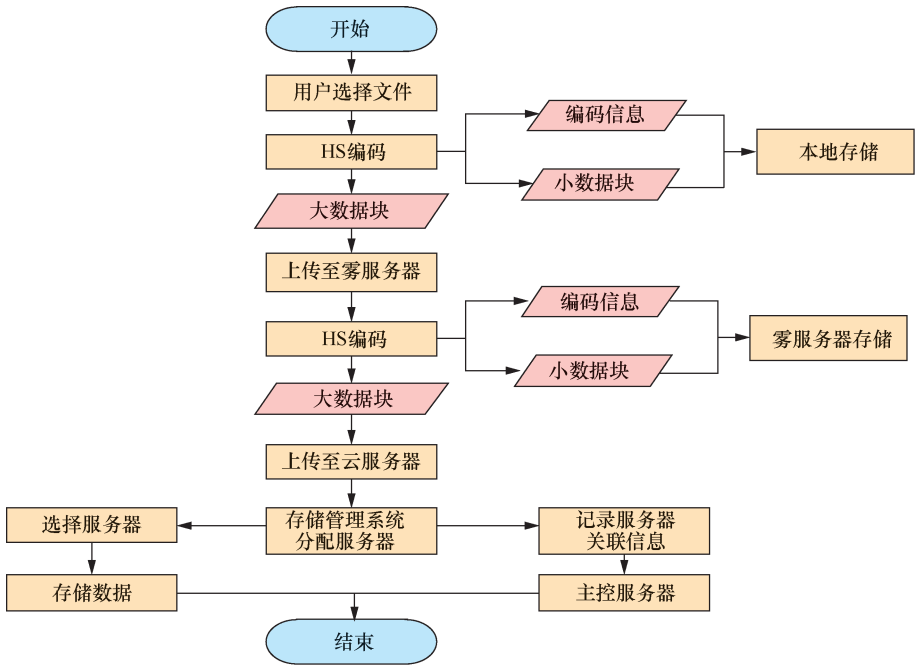

图 2　用户存储文件流程

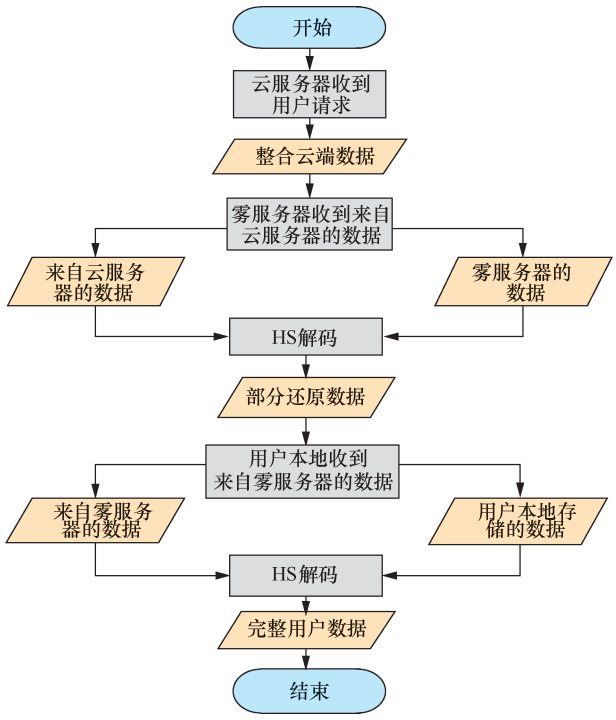

图 3　用户读取文件流程

3) 用户收到来自雾服务器的数据后，重复雾服务器步骤 2)的操作，根据存储在本地 RS 编码信息及部分数据，还原原始数据。

3.4　方案安全性理论分析

本节将对本文所提的结构进行安全性理论分析，证明该安全云存储架构可以改善传统安全云存储架构的隐私保护问题。

本文基于 RS 编码算法，提出 HS 编码算法。HS 编码过程实际上是散列变换加矩阵运算的过程，HS 编码过程如图 4 所示。首先将待存储数据 O 按字节映射到伽罗华域 GF(2^w)中[22]，进行散列变换后转换为 X 再与编码矩阵进行矩阵乘运算，产生相应数据分块 X_1~X_6 和冗余数据块 C，其中编码矩阵一般由单位矩阵和范德蒙矩阵构成。接着对 X_1~X_5 做相同操作，用于产生存储于雾服务器和云服务器的分块及冗余数据。HS 编码具有如下性质：假设原始数据被分为 k 份，使用$(m+k)\cdot k$ 的编码矩阵进行编码，编码后产生 m 份冗余，在 $k+m$ 份数据块中，任意不小于 k 份数据都可以结合编码矩阵进行逆运算还原原始数据；如果数据块数小于 k，则无法恢复原始数据。利用 HS 编码的上述性质，在本文提出的系统中，每次进行文件分级存储时，都将小于 k 份的数据块存储在高层，m 份与剩余的数据块存储在较低层（一般剩余的数据块份数不大，理论上最多不能超过 $k-m$ 份）。通过这种合理的分配后，云服务器、雾服务器和本地都存储了一定比例的数据，即使攻击者得到其中任意一个服务器的所有数据，也无法还原原始数据。HS 算法与传统 RS 算法的不同之处在于：前者对分块后的数据进行了进一步散列变换，保证了局部数据的隐私性，为高隐私保护需求的用户提供了更细粒度的隐私保护。通过

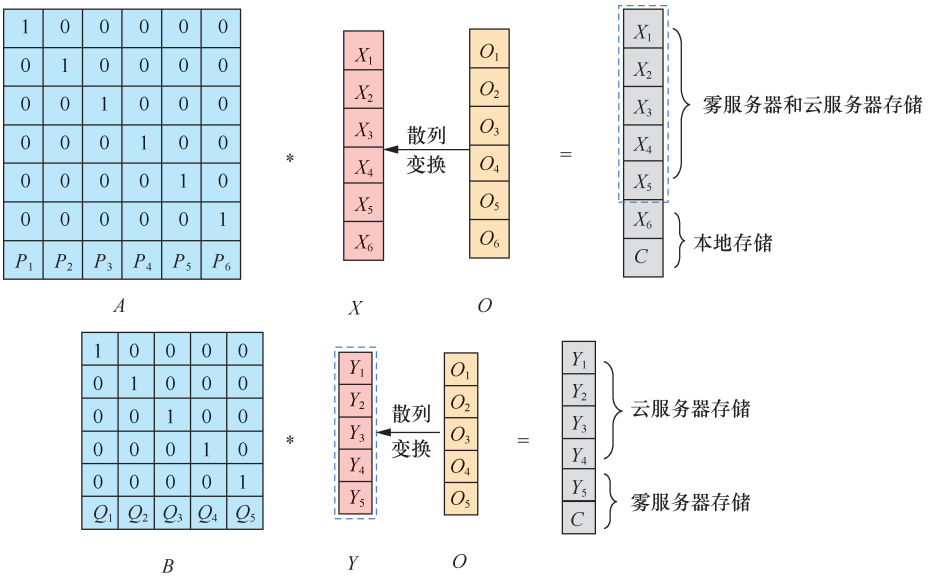

图 4　HS 编码过程

此方法在很大程度上杜绝了外来攻击者的非法获取或 CSP 窥探用户隐私的问题。进一步考虑更糟糕的情况，如果攻击者获取了两部分服务器的数据，则攻击者就拥有多于 k 份的数据，此时攻击者能否还原用户的原始数据就涉及编码矩阵的问题。攻击者获得所有数据后，如果没有编码矩阵中所包含的信息，则得到的依然是散乱的数据块，编码矩阵破解难度分析如表 1 所示。此外，编码矩阵的数据量较小，用户可以将其区别于普通数据进行重点保护，以免被攻击者盗取。

表 1　　编码矩阵破解难度分析

伽罗华域	m	k	穷举次数
GF(2^4)	1	6	256^3
GF(2^4)	2	6	256^6
GF(2^8)	1	6	256^6
GF(2^8)	2	6	256^{12}
GF(2^{16})	1	6	256^{12}
GF(2^{16})	2	6	256^{24}

从表 1 可以看出，即使只采用一个冗余数据块（m=1），攻击者也很难破解编码矩阵。而且在实际应用中，k 的取值较大，因此，编码矩阵在理论上是不可能被破解的。但是用编码分块并不能保证每个数据块中信息的隐私安全，如一个文档被分块后，每份数据块中仍包含部分文档信息，对于某些隐私性需求高的文件，显然无法满足需求。为了进一步保证数据安全性，在实际应用中和加密算法相结合，在 HS 编码中，数据块矩阵在和编码矩阵进行乘法运算前，先进行一次散列变换[23]，将原始数据序列打乱，同时将散列变换的相关信息保存在本地，在解码后利用这些信息对数据进行解密，进一步加强用户数据的私密性，避免攻击者读取片段的信息。

4　实验与分析

本文通过一系列测试评估所提的基于雾计算思想的三级安全云存储方案的性能与可行性，包括编码、解码及不同数据规模的多方面测试。

4.1　实验环境

实验环境如表 2 所示，用于测试的文件分别为图片、音频和视频。用于实验的文件分别为图片（NEF 格式，24.3 MB）、音频（MP3 格式，84.2 MB）和视频（RMVB 格式，615 MB）。

表 2　　实验环境

名称	属性
操作系统	Linux
CPU	Intel Core i7 2.50 GHz
内存	8 GB
硬盘	1 TB

4.2　实验结果与分析

本文实验采用多一块原则，即下层服务器只保留 m+1 份数据，通过这种方式，可以在保证数据私密性的前提下，尽量减小下层服务器的存储压力。

不同规模文件本地存储量变化如图 5 所示，对不同种类、大小的文件在该存储方案下的存储性能进行分析。在冗余数据块数量 $m = 2$ 的情况下，随着数据分块数 k 的增加，本地存储的数据量逐渐下降，这代表着数据分块数越多，则本地存储压力越小，存储成本越低。同时，不同大小的文件在存储中表现不同，文件越大，则在该方案下的表现越好。综上所述，在实际应用中，需要尽量增加 k 值以减少本地存储量，同时还要注意将较小的文件进行合并之后再存储。但数据分块数 k 并非越大越好，因为数据块数 k 越大，进行编码、解码处理的消耗越大。

数据分块数 k 与编码时间关系如图 6 所示，针对不同数据分块数 k 对该三级安全云存储系统性能的影响进行分析。由图 6 可以看出，随着数据分块数 k 的增加，原数据编码分块时间呈指数级上升。由于云存储系统是为用户服务的，过长的存储时延不能满足用户需求，因此在决定数据分块数 k 的取值时，应根据本地的机器性能进行动态更改。

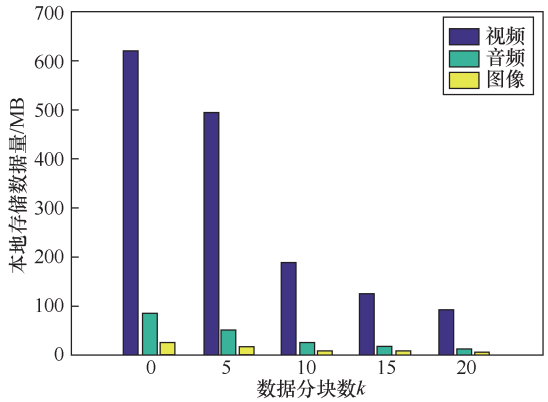

图 5　不同规模文件本地存储量变化

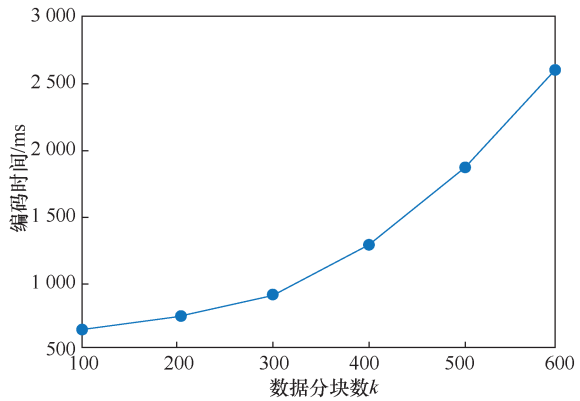

图 6　数据分块数 k 与编码时间关系

数据分块数 k 与解码时间关系如图 7 所示，与编码时间类似，数据分块数 k 影响解码时间。随着数据分块数的增加，解码恢复原始数据的时间也增加，体现在用户下载云中文件的速度，因此解码时间不能过大。在实际应用中，应结合编码性能和存储效率进行综合考虑。

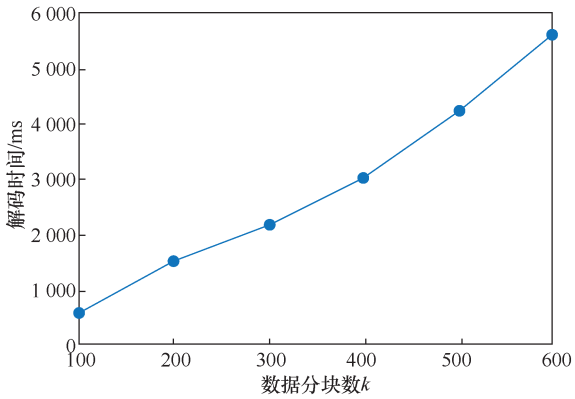

图 7　数据分块数 k 与解码时间关系

在解码阶段缺失不同数据块数量情况下，对本存储方案的性能影响进行分析。实验中冗余块数量 m=5、k=100，实际上 m 的取值和本地存储的数据总量大小有关，其值不能太大，否则将造成用户的存储负担过大。

在解码恢复原始数据时，使用至少 k 个数据块虽然可以恢复用户的原始数据，但会使得系统性能下降，不同丢失数据块数对解码时间的影响如图 8 所示。当丢失数据块数增加时，即解码时使用总数据块数量减少，解码时间随之增加，因此在进行解码时，最好把上层数据全部下载，以免增加下层服务器不必要的负担。

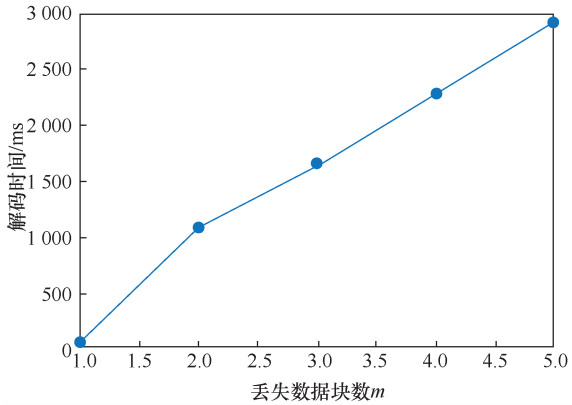

图 8　不同丢失数据块数对解码时间的影响

以上实验验证了编码/解码时间和数据分块数 k

之间的关系。但是系统架构并不仅考虑编码/解码时间，存储效率也是一个重要指标，存储效率表示为 $E_s=\frac{k}{k+m}$，而编码效率表示为 $E_c=\frac{\ln(k+m)}{\ln 2}$。在存储效率方面，考虑编码产生的冗余数据对数据的影响，因此，用原始数据块 k 和加上冗余数据块的总数据块数量 $k+m$ 相比。而编码效率则较复杂，编码效率直接正比关联于所选择的伽罗华域的字长 ω，根据 HS 编码的性质，$2^{\omega}<k+m$，因此可以将 ω 作为编码效率的指标，表示为 $\frac{\ln(k+m)}{\ln 2}$。存储效率与编码效率如图 9 所示，可以看出编码效率和存储效率成反比，因此在实际应用中面临一个问题，即如何选取合适的 k 值来平衡两者的矛盾，使系统达到综合的最佳效率。因此，设计了一个用于评估系统的均衡指标，$E_w=\mathrm{C}_1\frac{\ln(k+m)}{\ln 2}+\mathrm{C}_2\frac{k}{k+m}$，通过大量测试，最终取 C_1、C_2 两个常数分别为 0.6 和 0.4。系统综合效率示意图如图 10 所示，可以看出随着数据分块数 k 的增长，系统综合效率先增长后降低，

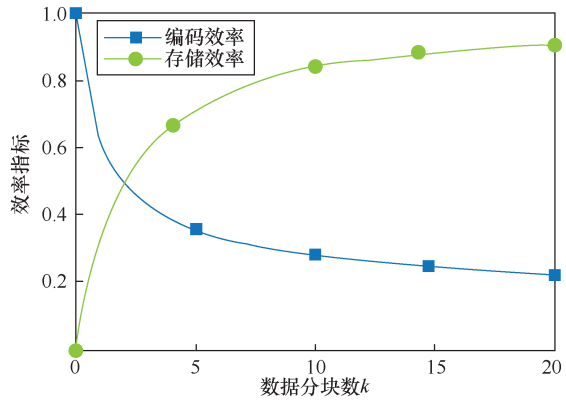

图 9　存储效率与编码效率

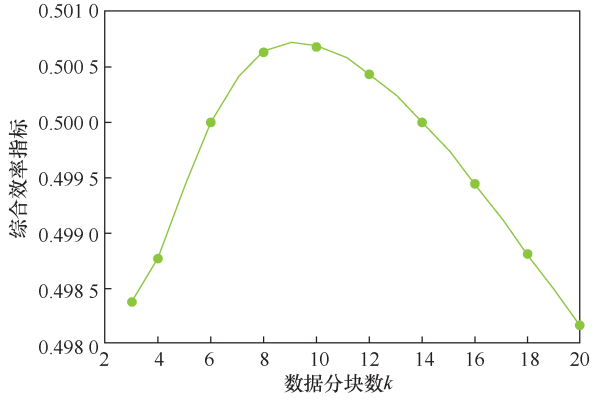

图 10　系统综合效率示意图

并在 k=10 附近达到极大值。因此在实际应用中，要通过类似方法找到最适合的 k 值，以保证系统的综合效率。

5　结束语

针对云存储的隐私问题，本文提出了基于雾计算思想的私密性云存储方案，给出了具体的解决方案，并通过安全性理论分析证明了该方案的隐私保护机制可行。通过合理分配云/雾服务器上存储的数据块比例，可以保证各个服务器数据的私密性；另一方面，攻击者若要破解编码矩阵，理论上是不可能的；此外，采用 HS 算法可以保证局部数据信息的私密性。通过实验测试表明，该方案可以在不影响云存储性能的情况下完成编码、解码工作。在现结构中，整体信息的顽健性依赖于本地数据的稳定性，因为如果本地存储的信息丢失，会导致用户原始数据无法还原，从而牺牲了云存储原本的数据备份、跨地/跨设备协调作用。在将来的研究中，要设计一种合理的、可以综合存储性能和私密保护性的模型用于评估不同分块数情况下系统的综合性能；另一方面，在编码技术上也将力图寻找更有效率并且具备隐私保护功能的编码方式；此外，将进一步完善系统结构，在保持云存储原有方便性的基础上，进一步提高系统安全性。

参考文献：

[1] MELL P, GRANCE T. The NIST definition of cloud computing[J]. Communications of the ACM, 2011, 53(6): 50.

[2] WANG T, XING G, LI M, et al. Efficient Wi-Fi deployment algorithms based on realistic mobility characteristics[C]//Mobile Ad hoc and Sensor Systems (MASS). IEEE, 2010: 422-431.

[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]. 计算机研究与发展, 2014, 51(7): 1397-1409.
LI H, SUN W H, LI F H, et al. Secure and privacy-preserving data storage service in public cloud[J]. Journal of Computer Research and Development, 2014, 51(7): 1397-1409.

[4] 肖亮, 李强达, 刘金亮. 云存储安全技术研究进展综述[J]. 数据采集与处理, 2016, 31(3): 464-472.
XIAO L, LI Q D, LIU J L. Survey on secure cloud storage[J]. Journal of Data Acquisition and Processing, 2016, 31(3): 464-472.

[5] MCELIECE R J, SARWATE D V. On sharing secrets and Reed-Solomon codes[J]. Communications of the ACM, 1981, 24(9): 583-584.

[6] PLANK J S. T1: erasure codes for storage applications[C]//The 4th USENIX Conference on File and Storage Technologies. USENIX, 2005: 1-74.

[7] 黄汝维, 桂小林, 余思, 等. 云环境中支持隐私保护的可计算加密方法[J]. 计算机学报, 2011, 34(12): 2391-2402.

HUANG R W, GUI X L, YU S, et al. Privacy-preserving computable encryption scheme of cloud computing[J]. Chinese Journal of Computers, 2011, 34(12): 2391-2402.

[8] BELLARE M, HOFHEINZ D, KILTZ E. Subtleties in the definition of IND-CCA: when and how should challenge decryption be disallowed[J]. Journal of Cryptology, 2015, 28(1): 29-48.

[9] 成春香, 张伟, 徐涛. 一种基于云存储的数据安全与隐私保护系统[J]. 北京信息科技大学学报(自然科学版), 2013(2): 87-90.
CHENG C X, ZHANG W, XU T. A data security and privacy protection system based on cloud storage[J]. Journal of Beijing Information Science and Technology University, 2013(2): 87-90.

[10] 侯清铧, 武永卫, 郑纬民, 等. 一种保护云存储平台上用户数据私密性的方法[J]. 计算机研究与发展, 2011, 48(7): 1146-1154.
HOU Q H, WU Y W, ZHENG W M, et al. A method on protection of user data privacy in cloud storage platform[J]. Journal of Computer Research and Development, 2011, 48(7): 1146-1154.

[11] BARHAM P, DRAGOVIC B, FRASER K, et al. Xen and the art of virtualization[C]//ACM SIGOPS Operating Systems Review. ACM, 2003, 37(5): 164-177.

[12] SHEN J, SHEN J, CHEN X F, et al. An efficient public auditing protocol with novel dynamic structure for cloud data[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(10): 2402-2415.

[13] SHEN J, LIU D Z, SHEN J, et al. A secure cloud-assisted urban data sharing framework for ubiquitous-cities[J]. Pervasive Mobile Computing, 2017(41): 219-230.

[14] 傅颖勋, 罗圣美, 舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展, 2013, 50(1): 136-145.
FU Y X, LUO S M, SHU J W. Survey of secure cloud storage system and key technologies[J]. Journal of Computer Research and Development, 2013, 50(1): 136-145.

[15] BHUIYAN M Z A, WANG T, HAYAJNEH T, et al. Maintaining the balance between privacy and data integrity in Internet of things[C]//The 2017 International Conference on Management Engineering, Software Engineering and Service Sciences. ACM, 2017: 177-182.

[16] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the Internet of things[C]//Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. ACM, 2012: 13-16.

[17] STOJMENOVIC I, WEN S. The fog computing paradigm: scenarios and security issues[C]//Computer Science and Information Systems (FedCSIS). IEEE, 2014: 1-8.

[18] 曾建电, 王田, 贾维嘉, 等. 传感云研究综述[J]. 计算机研究与发展, 2017, 54(5): 925-939.
ZENG J D, WANG T, JIA W J, et al. Survey of sensor-cloud[J]. Journal of Computer Research and Development, 2017, 54(5): 925-939.

[19] 王田, 李洋, 贾维嘉, 等. 传感云安全研究进展[J]. 通信学报, 2018, 39(3): 35-52.
WANG T, LI Y, JIA W J, et al. Research on security of sensor-cloud[J]. Journal of Communication, 2018, 39(3): 35-52.

[20] LAI Y X, XIE J S, LIN Z Y, et al. Adaptive data gathering in mobile sensor networks using speedy mobile elements[J]. Sensors, 2015, 15(9): 23218-23248.

[21] WANG T, LI Y, WANG G J, et al. Sustainable and efficient data collection from WSNs to cloud[J]. IEEE Transactions on Sustainable Computing, 2017: 1.

[22] BERLEKAMP E R. Galois field computer: US4, 162, 480[P]. 1979.

[23] BAKHTIARI S, SAFAVI-NAINI R, PIEPRZYK J. Cryptographic hash functions: a survey[J]. Centre for Computer Security Research, 1995(4): 95-109.

[作者简介]

周际援（1994− ），男，安徽蚌埠人，华侨大学硕士生，主要研究方向为雾计算、安全云存储。

罗皓（1994− ），男，广东惠州人，华侨大学硕士生，主要研究方向为无线传感网络、移动计算以及雾计算。

邱磊（1993− ），男，湖北十堰人，华侨大学硕士生，主要研究方向为无线传感网络、移动计算以及雾计算。

王田（1982− ），男，湖南汨罗人，博士，华侨大学教授、硕士生导师，主要研究方向为无线传感网络、移动计算以及雾计算。