对云上的加密数据进行安全搜索的技术的调查

刘园春

摘要：

云计算已成为企业和个人将数据外包给远程但高度可访问的服务器的潜在资源。但是，由于用户担心数据隐私和安全性，因此尚未完全实现云服务的潜力。可以采用用户方加密技术来减轻安全问题，但是一旦对数据进行加密，就不能对外包数据执行任何处理（例如，搜索）。已经对可搜索加密（SE）技术进行了广泛的研究，以在对数据进行加密时进行搜索。这些技术可以对加密数据进行各种类型的搜索，并提供不同级别的安全性。尽管这些技术支持不同的搜索类型并在细节上有所不同，但它们在组件和体系结构上具有相似之处。在本文中，结合相关文献提供了有关不同安全搜索技术的相关调查，分析了这些系统的体系结构和该领域的未来研究方向。

关键词：云安全，加密搜索，加密数据搜索，调查

1 前言

云计算因其众多优势而受到青睐，包括便利性和可访问性，一致的备份以减轻本地存储的负担以及节省内部硬件和软件维护的资本支出。[1]但是，公共云存储服务可能会被多方使用。租户客户，这些客户在云上存储了大量潜在的敏感数据。使用云存储意味着失去对数据的完全控制权，并将其委派给云管理员，使数据遭受潜在的外部和内部攻击[2,3]，这对于依赖于其数据机密性的组织（例如金融公司）而言是毁灭性的。

这些问题使企业担心将其数据外包到云中并利用其潜力。[4,5]例如，由于法律法规的约束，拥有患者健康记录的医疗中心无法将其数据外包到容易受到攻击的云中。[6]在另一种情况下，出于类似的考虑，保留敏感犯罪记录的执法机构会犹豫使用云存储。

解决机密性问题的一种方法是在将本地数据加密后再将其外包给云。尽管此方法可以保护数据机密性，但会妨碍数据处理。特别是对于外包的非结构化数据而言，搜索至关重要。[7]实际上，当对数据进行加密时，搜索系统不再起作用，因为它们无法将查询与加密数据进行比较。

Song 等人[8]的工作可以追溯到 2000 年，创建可搜索加密系统的工作从那时起，为了实现不同类型的可搜索加密，已经进行了大量研究工作。尽管这些系统在搜索方法，安全级别和性能上有所不同，但它们在某些体系结构上具有相似之处。还有其他针对不同可搜索加密系统的调查研究。[9,10]

本文的其余部分安排如下。第 2 节介绍了可搜索加密的背景和初步知识。第 3 节给出了可搜索加密的总体框架。第 4 节回顾了不同的可搜索加密方案的分类。第 5 节结合相关文献中作者的研究成果总结了一些该领域未来可能的研究方向。最后，第 6 节总结了本文。

2 基于云的可搜索加密系统的要素

Song 等人[8]是可搜索加密的先驱之一。他们提供了一个系统，客户端（即数据所有者）可以在电子邮件服务器上搜索其加密数据（以电子邮件的形式）。数据所有者一旦要在电子邮件中搜索某些关键字，便向服务器提交加密的查询（称为活板门）。服务器负责搜索加密数据并检索所有者的相关电子邮件。可搜索加密的最新研究著作（例如其他著作[11,12]）描述了其系统具有与此著作相似的元素。我将在本节接下来的部分中更详细地介绍这些元素。

如图 1 所示，受 Sun 等人和 Saleem 等人[11]的启发，可搜索的加密系统通常由以下三个主要元素组成。

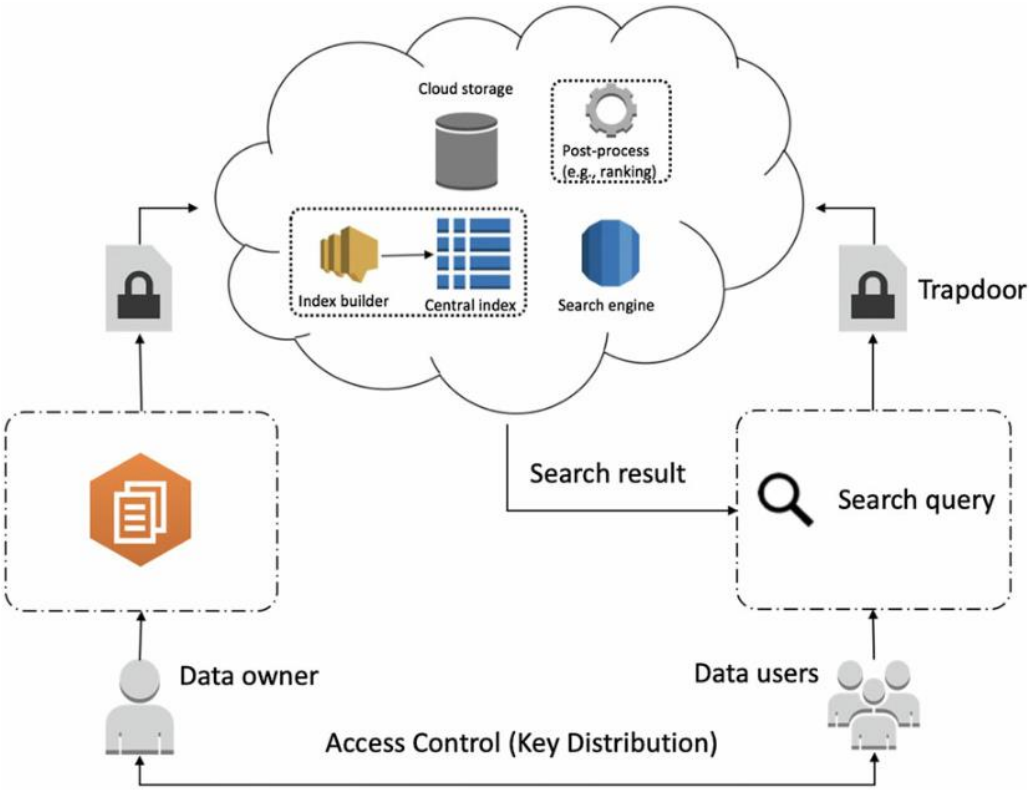

图 1 基于云的可搜索加密系统涉及的主要元素

数据所有者。数据所有者通过授予对数据用户的访问权限并将文件上传到云来设置系统。数据所有者拥有 n 个文档 D = {d_1，d_2，…，d_n} 的集合，并希望将它们外包给远程公共云服务器（例如 Amazon 和 IBM Cloud Storage）以进行存储或共享。为了保护文档的机密性，所有者使用其授权密钥在本地对数据进行加密，然后将加密的数据上传到云中。

数据用户。数据用户是有权搜索和检索上载文档的用户。数据用户具有一个加密密钥，该加密密钥将应用于他们的搜索查询以创建陷阱门。陷阱门然后被发送到云服务器以相关文档列表的形式检索搜索结果（例如，在 Cao 等人的著作中[13]和 Fu 等人的著作中[14]）或文档标识符。实际上，数据所有者也可以是数据用户。

云服务器。云服务器接收由数据所有者上传的加密文档集合，并执行三个主要任务：存储上传的文档，在活板门中搜索它们以及维护和更新相关的数据结构。在基于云的可搜索加密中进行的研究工作通常都假定云服务器是诚实而又好奇的。也就是说，尽管云服务器管理员遵循了必要的安全程序，并且没有修改或删除数据文件，但她仍然对文档的内容“感到好奇”。

3 可搜索加密系统的一般架构

可搜索加密系统的体系结构必须实现与上一节中提到的元素有关的四个过程。在本节中，将首先描述这四个过程，然后讨论它们如何在可搜索加密系统的不同元素中应用。

3.1可搜索加密系统中涉及的过程

可搜索的加密系统中的过程是密钥生成（Keygen），构建索引，Trapdoor 生成和搜索。这些过程启用了可搜索的加密系统，并且通常具有多项式时间复杂度。[15]

密钥生成(Keygen)过程。此过程创建一个密钥来加密纯文本文档，然后再解密检索到的文档。此过程的算法根据一组给定的安全参数生成密钥。概率密钥生成算法[15]通常用于此过程。

随着数据所有者和用户通过服务器传输和存储数据，需要安全地存储文档并确定用户是否有权访问它们。有两种常用的文档加密方法，即对称加密和非对称加密。

对称加密：在这种方法中，数据所有者和数据用户都共享相同的密钥。此密钥可用于加密和解密文档。换句话说，此密钥将在文档中产生噪音，从而使未经授权的用户无法读取它们，而授权用户可以使用该共享密钥（或可计算的“反向”密钥）来消除和消除文档中的噪音。[16]

非对称加密：称为公钥加密。该密码术包括两个不同的密钥，公钥和私钥，用于加密和解密文档。更具体地说，数据所有者将使用他的一个密钥来加密文档，而使用另一个来解密。由于这两个密钥完全不同，并且它们之间没有计算相关性，因此即使加密密钥（公钥）遭到破坏，如果没有私钥，攻击者也无法获取数据内容。

建立索引。可搜索的加密系统通常利用索引结构来跟踪文档中关键字的出现。初始化此索引的过程称为 Build-Index，由 Keygen 处理，然后将文档 D 的集合作为输入。然后，它从文档中提取关键字并将其插入索引结构。

数据所有者使用此构建索引过程来生成安全且可搜索的结构，从而可以对加密的数据进行搜索。索引结构通常以哈希表，[17]元数据(标记)，[11]或倒排索引[18]的形式实现。对于每个出现的文档，索引都映射到标识符。

活板门一代。数据用户使用此过程来形成搜索查询。它使用与 Build-Index 密钥 K 兼容的密钥对用户的搜索查询进行加密。如果需要，将通过 Trapdoor 生成过程对搜索查询进行预处理（例如，扩展）。[19]然后，将加密的 Trapdoor 进行加密。发送到云服务器。

搜索。收到陷阱门后，服务器将运行搜索过程以匹配包含陷阱门中的关键字集的文档。接下来，将结果发送回客户端。

3.2可搜索加密系统的通用体系结构

系统体系结构由两个主要机制组成，即设置和检索。设置机制的主要工作是准备要由数据用户搜索的文档。接收到来自数据用户的搜索查询后，检索机制的工作是对数据集执行搜索，找到匹配的文档，然后将结果发送回数据用户。在下一节中，将详细介绍这些机制的运作方式。

3.2.1 建立机制

在将文档发送到云之前，安装程序机制首先从文档中提取有用的信息。提取的数据的类型取决于搜索系统的类型（例如，关键字搜索与语义搜索）。然后，提取的数据和文档被加密并发送到云服务器。

数据所有者通过 Keygen 流程启动搜索系统。生成的密钥对于在外包之前加密文档和解密下载的文档是必需的。

在某些可搜索的加密系统中，设置机制还包括创建“索引结构”.[20]索引结构也称为“元数据”[11]或“识别关键字”。索引由代表每个上载文档本质的关键字组成。或者，其他一些可搜索的加密系统不依赖于索引结构，而是直接对每个关键字进行单独加密以形成加密的可搜索文档。[8]

然后，可搜索的加密系统将文档的内容以及索引结构（如果存在）加密，然后再将其发送到云服务器。

在数据所有者和数据用户是独立实体的系统中，数据所有者需要将公钥分配给数据用户。数据用户使用密钥来创建与加密的上载数据兼容的活板门。公钥加密[17]或广播加密等方法通常用于密钥分发。

3.2.2 检索机制

设置完成后，系统将准备好要搜索的文件集合。数据用户或所有者可以提交搜索查询，该查询定义为一组关键字 W = {w_1，w_2，…，w_n}。

陷阱门是使用 W 和数据所有者的键生成的。一些系统（例如，Cao 等人[13]和 Xia 等人[21]的作品）在生成活板门时也对搜索查询进行了预处理。产生后，将其发送到云服务器。

云服务器包括执行搜索过程的搜索引擎。在依赖索引结构的系统中，索引用于将 Trapdoor 与索引条目进行匹配以查找相关文档。最后，结果列表（包括匹配的文档或其标识符）被发送回用户。接收到结果列表后，数据用户可以请求检索（即下载）和解密文档（如果已授权）。

在检索机制期间，云服务器可以学习有关文档的最少信息。

4 可搜索加密系统的分类

已经进行了各种研究努力以对加密数据进行不同形式的搜索操作。但是，许多这些努力都植根于一些通用方法。本部分的目的是提供当前可搜索加密系统的全面分类法，并概述该领域中进行的研究。图 2 提供了可搜索加密系统的分类。从该图可以看出，可搜索加密系统可以根据其执行的搜索类型大致分为以下三种类型：关键字搜索，正则表达式搜

索，和语义搜索。

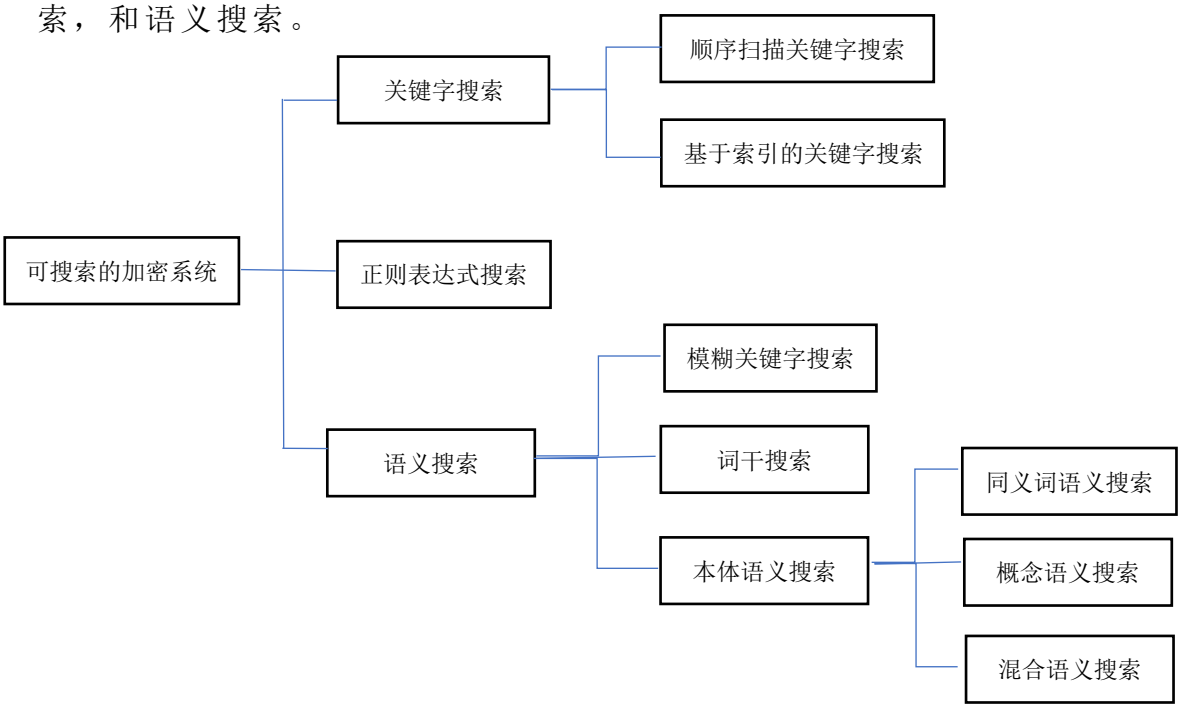

图 2 当前可搜索加密系统的分类

4.1 关键字搜索

4.1.1 顺序扫描关键字搜索

Song 等人[8]提出了用户端加密和对加密文档进行基于关键字的搜索的想法。用户打算检索包含她的搜索关键字的加密文档。在提出的方案中，文档的每个关键字W_i在两个加密层中被独立加密。首先，他们将关键字W_i和 E（W_i）预加密为 n 位。然后将其分为两部分，即，右侧部分（R_i）由 m 位组成，而左侧部分（L_i）由 n-m 位组成。

其次，使用流密码对左侧部分进行加密，可以使用 XOR 检查是否匹配。当用户请求包含一组感兴趣的关键字的文档时，她提交查询中每个关键字的加密版本，即L_i和k_i；服务器对每个密文的 n-m 位执行 XOR 匹配，以查看是否对某些 S[8]的形式为（S，F_ki（S））的C_i XOR L_i。在此系统中，由于每个单词均被独立加密，因此可以找到所有匹配项，服务器必须对整个文档逐个单词地遵循上述步骤。因此，这种搜索方法称为顺序扫描。

由于在整个数据集中进行搜索的时间复杂度有限，并且数据集的数量在不断增长，因此没有多少主流研究工作遵循这种方式。稍后将提到更高级和有效的可搜索加密系统。

4.1.2 基于索引的关键字搜索

早期的工作[8]使用基于索引的关键字搜索及其自己的方法来对加密文档执行单个关键字或析取关键字搜索。但是，随着数据用户需求的增长，需要更准确的搜索结果，将不同的技术引入索引以支持多关键字

和联合关键字搜索。 MRSE49 是为该需求提出解决方案的第一批作品之一。 Cao 等人[13]定义了一个包含所有关键字的字典，每个关键字在字典中都有定义的位置。数据文件和搜索查询由二进制矢量表示，然后使用“内部乘积计算”来衡量数据文件和查询的相似性。Cao 等人[13]也运用自己的内部排名返回相关的有序结果。后来，Xu 等人[22]改进了 MRSE，因此可以动态扩展其固定字典。他们的工作还通过使用访问频率加权匹配的数据文件来改进排名算法。

4.2 正则表达式搜索

基于关键字的可搜索加密的一种扩展是允许用户对加密的数据执行正则表达式搜索。Song 等人[8]的初步方法建议创建给定正则表达式的所有可能变体。例如，对于查询 ab [a-z]，它将生成所有 26 个可能的搜索查询，即 aba，abb，…，abz。这种方法仅适用于简单的正则表达式，而对于具有高度可变性（例如a^*b^*）的表达式则不可扩展。

RESeED[23]是用于加密数据的正则表达式搜索系统。 RESeED 基于两个数据结构进行操作，即列存储，它是未加密的反向索引，表示关键字及其出现的文档；订单存储，它是文档中关键字的模糊（哈希）表示。对于给定的搜索词组，RESeED 建立一个不确定的有限自动机（NFA）。然后，NFA 划分为子 NFA，可以与列存储中的关键字匹配。对于上一步中找到的文档，将检查其订单存储以确认关键字与正则表达式的顺序相同。

4.3 语义搜索

当用户完全知道他们在文档中搜索的关键字时，提供基于关键字或基于正则表达式的搜索功能的可搜索加密解决方案将非常有用。但是，随着文档收集的增加和大数据的出现[24]，数据用户可能不记得他们想要检索的确切关键字，或者他们可能想搜索与主题更广泛相关的文档。[18]

例如，在具有加密病历的医院中，医生可能希望使用查询“心脏病”来搜索记录。虽然医生对包含确切查询字词的文档感兴趣，但她对语义上也很感兴趣的文档相关术语（例如“心脏病发作”或“胸痛”）。因此，需要进行语义搜索以返回与查询中的术语相关的文档，并避免重复的搜索尝试。

已经进行了许多研究工作以实现不同形式的语义可搜索加密。如我们在分类法中看到的（图 2），这些语义搜索系统可以进一步分为三种主要类型，即模糊关键字搜索，词干搜索和本体搜索。

4.3.1 模糊搜索

如果模糊关键字搜索未能为精确查询找到足够的匹配项，则通过搜索与查询的紧密匹配项来提高系统的可用性。尽管这些系统被归类为搜

索系统，但它们可能不会直接用于搜索目的。模糊搜索可用于使系统能够容忍用户的错字[25]。

模糊关键字搜索系统基于测量两个字符串s_1和s_2[26]之间相似度的编辑距离来工作。编辑距离定义为将s_1转换为s_2所需的字符串操作数。可能的字符串操作是插入（将字符插入字符串），替换（将一个字符替换为字符串中的另一个字符）和删除（从字符串中删除字符）。让 D = {d_1，d_2，…，d_n} ，是存储在不受信任的第三方服务器（例如云）上的文档的集合； W = {w_1，w_2，…，w_n}是具有固定编辑距离 d 的一组唯一关键字；以及（s，k）阈值 k≤d 的搜索活板门。然后，模糊关键字搜索系统输出可能包含关键字 w，如果 w∈W 的文档列表；否则，返回 ed（w，w_i）< k。

在模糊关键字搜索中，系统需要搜索模糊关键字的整个列表，这对于较大的编辑距离会产生大量开销。因此，为进一步提高模糊搜索性能，Wang 等人[27]从模糊关键字集中构建了一棵树，将搜索结果减少为模糊列表大小的 O（log（n））。

4.3.2 词干搜索

使用模糊关键字搜索使可搜索的加密系统更能抵抗较小的拼写错误，但在许多情况下并不能完全涵盖语义方面。尽管具有较大的编辑距离（4），但不同的单词（例如，“学生”和“学习”）在语义上高度相关。词干搜索方法旨在基于以下信念来解决此问题：与语义相关的单词倾向于从相同的词根（词干）开始。

该模型与其他可搜索的加密系统相同，即，用户加密文档并提取关键字作为加密索引。该系统的不同之处在于，将关键字集转换为一组词干需要执行额外的步骤。当用户搜索查询时，每个查询关键字都由其词干替换。

上传的文档和搜索查询扩展都经过相同的过程来获取提取的关键字的词干。这些词干关键字存储在第三方服务器（例如，公共云）的索引中，并在搜索过程中使用。

4.3.3 本体语义搜索

模糊关键字和词干可搜索加密方法无法真正捕捉搜索中的语义本质。例如，如果用户打算搜索抢劫案，那么她可能也有兴趣查看有关“入室盗窃”或“闯入”的结果。但是，模糊关键字和词干提取方法都无法捕获这种类型的语义。实际上，与语义相关的词既没有相同的词干，也没有密切的编辑距离。为了解决这个问题，发明了本体语义搜索来查找与原始查询更有意义的相关数据。[18]正如在图 2 的分类法中看到的那样，可以使用同义词语义，概念语义或混合语义来实现本体语义搜索。这些语义的组合。在这一部分中，我将探讨这些方案。但是，首先回顾一些可以进行本体搜索的初步概念。

语义关系：心理语言学家，丘奇和汉克斯[28]提出，可以从对这些词的共现定义的词之间的语义关系的统计描述中推断出词的关联。为了计算两

个关键字之间的相似度得分，Sun 等人使用了数据挖掘方法来有效地找出数据集中各个词之间的共现度。对于两个字符串 x 和 y，基于等式（1）定义相似性得分信息 I(x,y)。

$$I(x,y) = \log_2\left(\frac{P(x,y)}{p(x)p(y)}\right) \quad (1)$$

其中 P（x，y）是 x 和 y 一起出现的概率，而 p（x）和 p（y）是 x 和 y 在集合中独立出现的概率。相似性评分的值越高，表示 x 和 y 之间的相关性越高。

Woodworth 等人[29]提出了一项工作，该工作通过仅从上载文档中提取最重要的术语来减少索引中的术语数量，并使用 Wikipedia 和 Synonyms 扩展查询以捕获查询的更广泛含义。结果是节省空间的索引，该索引仍然可以实现准确的语义搜索。

5 未来研究方向

在本节中，结合相关文献，假设设想的各种方向都是必需的，可搜索加密领域的研究人员可能会发现他们的兴趣。这些主题中的每一个甚至什至是多个建议的组合都可能推动可搜索加密继续向前发展。

可用于搜索加密的边缘计算。ENSURE 是基于边缘计算的可搜索加密系统架构。[30]它介绍了一种通过移动设备提供可搜索加密系统功能的方法。这是通过将繁重的任务外包给边缘设备，将最终设备从繁重的计算工作中释放出来并节省能源来实现的。该文还通过依赖边缘设备而不是公共（云）服务器的可信度来提高安全性。

集群加密数据。Chen 等人[31]提出了一种将加密数据分布和排列到有意义的簇中的新功能。通过将亲和力传播和 K-means 聚类方法相结合，称为 CAK-means 模型，它们可以将相关数据划分为一定数量的簇。该模型保持相关数据文件的紧密性，并支持 I / O 操作，从而进一步改善了上传过程和整个系统。

跨多源数据集的可搜索加密。[32]数据集还可能具有不同的特征，例如文档结构或长度。需要进一步研究以处理更广泛的数据，并结合多个安全级别。遵循此方向的最新工作之一是来自 Guo 等人[33]的工作，他们建立了一个可信客户端在服务器节点集群上发出查询的场景。他们提出了 EncKV，这是一种存储加密数据并支持使用标准数据分区算法的丰富查询检索的系统。为了在分布式数据存储中提供丰富的查询，客户端维护一个小的哈希结构来跟踪元数据。

6 总结

在这项工作中，我调查了当前可搜索的加密系统和技术，结合相关文献归纳了该方面的相关知识，并且分析了可搜索加密系统的体系结构。最后，我根据相关文献，总结了这方面未来可能的研究方向，包括利用边缘计算，对数据进行聚类以提高搜索速度，以及跨多个数据集进行搜索。

参考文献

1. Avram M-G. Advantages and challenges of adopting cloud computing from an enterprise perspective. Procedia Technology. 2014;12:529-534.
2. Yan Z, Li X, Wang M, Vasilakos AV. Flexible data access control based on trust and reputation in cloud computing. IEEE Trans Cloud Comput.2017;5(3):485-498.
3. Sohal AS, Sandhu R, Sood SK, Chang V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur. 2018;74:340-354.
4. Nakayama M, Chen C, Taylor C. The effects of perceived functionality and usability on privacy and security concerns about cloud application adoptions. J Inf Syst Appl Res. 2017;10(2):529-534.
5. Chang V, Kuo Y-H, Ramachandran M. Cloud computing adoption framework: a security framework for business clouds. Futur Gener Comput Syst. 2016;57:24-41.
6. Singh J, Pasquier T, Bacon J, Ko H, Eyers D. Twenty security considerations for cloud-supported Internet of Things. IEEE Internet Things J.2016;3(3):269-284.
7. Meharwade A, Patil GA. Efficient keyword search over encrypted cloud data. Procedia Comput Sci. 2016;78(C):139-145.
8. Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P); 2000; Berkeley, CA.
9. Bösch C, Hartel P, Jonker W, Peter A. A survey of provably secure searchable encryption. ACM Comput Surv. 2014;47(2):18:1-18:51. http://doi.acm.org/10.1145/2636328
10. Poh GS, Chin JJ, Yau WC, Choo KKR, Mohamad MS. Searchable symmetric encryption: designs and challenges. ACM Comput Surv. 2017;50(3):40:1-40:37. http://doi.acm.org/10.1145/3064005
11. Saleem M, Warsi MR, Khan NS. Secure metadata based search over encrypted cloud data supporting similarity ranking. Int J Comput Sci Inf Secur.2017;15(3):353-361.
12. Ali N, Pathan N, Dubey SP. Privacy and protection of mobile health data on secure cloud storage. Imp J Interdiscip Res. 2017;3(4).
13. Cao N, Wang C, Li M, Ren K, Lou W. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans Parallel Distributed Syst. 2014;25(1):222-233.
14. Fu Z, Sun X, Liu Q, Zhou L, Shu J. Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Trans Commun. 2015;98(1):190-200.
15. Ballard L, Kamara S, Monrose F. Achieving efficient conjunctive keyword searches over encrypted data. In: Information and Communications Security:7th International Conference, ICICS 2005, Beijing, China, December 10-13, 2005. Proceedings. Berlin, Germany: Springer-Verlag Berlin Heidelberg;2005:414-426.
16. Fu Z, Ren K, Shu J, Sun X, Huang F. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans Parallel Distributed Syst. 2016;27(9):2546-2559.
17. Cash D, Jaeger J, Jarecki S, et al. Dynamic searchable encryption in very-large databases: data structures and implementation. In: Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS); 2014; San Diego, CA.

18. Woodworth JW, Amini Salehi M. S3BD: secure semantic search over encrypted big data in the cloud. Concurrency Computat Pract Exper. 2018.
19. Fu Z, Huang F, Ren K, Weng J, Wang C. Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data.IEEE Trans Inf Forensics Secur. 2017;12(8):1874-1884.
20. Wang C, Cao N, Ren K, Lou W. Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Trans Parallel Distributed Syst.2012;23(8):1467-1479.
21. Xia Z, Wang X, Sun X, Wang Q. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distributed Syst. 2016;27(2):340-352.
22. Xu Z, Kang W, Li R, Yow K, Xu CZ. Efficient multi-keyword ranked query on encrypted data in the cloud. In: Proceedings of the 2012 IEEE 18th International Conference on Parallel and Distributed Systems; 2012; Singapore.
23. Salehi MA, Caldwell T, Fernandez A, et al. RESeED: a secure regular-expression search tool for storage clouds.Softw Pract Exper. 2017;47(9):1221-1241.
24. Zobaed S, Amini Salehi M. Big Data in the Cloud. In: Sakr S, Zomaya A, eds. Encyclopedia of Big Data. Cham, Switzerland, Germany: Springer International Publishing; 2018.
25. Fu Z, Wu X, Guan C, Sun X, Ren K. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Forensics Secur. 2016;11(12):2706-2716.
26. Wang B, Yu S, Lou W, Hou YT. Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In: Proceedings of the IEEE Conference on Computer Communications (INFOCOM); 2014; Toronto, Canada.
27. Wang J, Ma H, Tang Q, et al. Efficient verifiable fuzzy keyword search over encrypted data in cloud computing. Comput Sci Inf Syst. 2013;10(2):667-684.
28. Church KW, Hanks P. Word association norms, mutual information, and lexicography. Computational Linguistics. 1990;16(1):22-29.
29. Woodworth J, Salehi MA, Raghavan V. S3C: an architecture for space-efficient semantic search over encrypted data in the cloud. In: Proceedings of 5th IEEE International Conference on Big Data (Big Data); 2016; Washington DC.
30. Guo Y, Liu F, Cai Z, Xiao N, Zhao Z. Edge-based efficient search over encrypted data mobile cloud storage. Sensors. 2018;18(4):1189.
31. Chen L, Zhang N, Li K-C, He S, Qiu L. Improving file locality in multi-keyword top-k search based on clustering. Soft Computing. 2018;22(9):3111-3121.https://doi.org/10.1007/s00500-018-3145-6
32. Fathi R, Salehi MA, Leiss EL. User-friendly and secure architecture (UFSA) for authentication of cloud services. In: Proceedings of the 8th International Conference on Cloud Computing (Cloud); 2015; New York, NY.
33 . Guo Y , Yuan X , Wang X , Wang C , Li B , Jia X . Enabling encrypted rich queries in distributedkey - valuestores . IEEE Trans Parallel Distributed Syst. 2018.