一种面向耗材数据的可搜索对称加密方案

景义君,程钰雯,时自成,任 莹,荆长强,郭 锋,武传坤
(临沂大学 信息科学与工程学院,山东 临沂 276000)

摘 要:目前将数据上传至公共服务器或云平台已成为系统管理数据的主流方法,然而这种做法存在着机密数据泄露和隐私泄露的严重风险。为了解决这一问题,保护数据的安全性和用户的隐私性,该文提出一种面向耗材数据的安全高效的可搜索对称加密方案,在耗材管理系统中提供了有效的数据保护和用户隐私保护措施。可搜索对称加密技术是一项能够在密文状态下实现搜索的先进技术,它允许在加密的数据集中进行搜索而无需解密。文章具体方案采用了 KECCAK256 哈希算法和 AES 加密算法对耗材数据进行处理,并引入倒排索引结构以及乱序操作来实现密文搜索功能。这种结构不仅能够有效地支持快速搜索,还能防止通过索引推断出明文信息,从而提高耗材数据的隐私保护水平。实验结果表明,该方案相较于其他算法在安全性和搜索时间方面均表现优异,为耗材管理系统提供了可靠且高效的数据的隐私保护措施。

关键词:隐私保护;耗材数据;可搜索对称加密;密文搜索;倒排索引
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2024)12-0081-06
doi:10.20165/j.cnki.ISSN1673-629X.2024.0262

A Searchable Symmetric Encryption Scheme for Consumable Data

JING Yi-jun, CHENG Yu-wen, SHI Zi-cheng, REN Ying, JING Chang-qiang,
GUO Feng, WU Chuan-kun
(School of Information Science and Engineering, Linyi University, Linyi 276000, China)

Abstract: At present, uploading data to public servers or cloud platforms has become the mainstream method for data management. However, this practice has serious risks of confidential data leakage and privacy leakage. In order to solve this problem and protect data security and user privacy, we propose a secure and efficient searchable symmetric encryption scheme for consumables data, which provides effective data protection and user privacy protection measures in the consumable material management system. Searchable symmetric encryption is an advanced technology that can realize search in ciphertext state, which allows searching in encrypted data sets without decryption. The proposed scheme uses the KECCAK256 hash algorithm and AES encryption algorithm to process data of consumable material management, and introduces an inverted index structure and random operation to realize the ciphertext search function. This structure can effectively support fast search, and can prevent the plaintext information from being inferred from the index, thereby improving the privacy protection level of the data. Experimental results show that compared with some known such algorithms, the proposed scheme performs well in terms of security and search efficiency, providing a reliable and efficient data privacy protection measure for the consumables management system.

Key words: privacy protection; consumable data; searchable symmetric encryption; ciphertext search; inverted index

0 引 言

随着信息技术的持续发展,耗材管理工作也走向数字化和信息化,特别是高等院校和研究机构,实验中往往需要大量耗材[1]。在耗材管理工作中,传统手工管理方式具有效率低和准确率低等问题,不能满足新时代的需求。为提高管理效率和错误率,将信息化引入耗材管理中形成智能化管理系统,解决人工和非移动的耗材仓储管理的弊端[2]。管理物品耗材是现代企业和学校等组织中的重要部分,它直接关系到参与者的利益和效率,例如对于学校耗材,师生购入的指定物品以及填报项目名称往往会体现该师生参与了怎样的项目课题,为防止耗材信息的泄露,以及耗材使用者身份的泄露,对耗材管理增加隐私保护功能是有必要的。为了更好地应用智能耗材管理系统,保护参与者的利

收稿日期:2024-05-24 **修回日期**:2024-09-25
基金项目:国家自然科学基金青年基金(61901206)
作者简介:景义君(2000-),女,硕士研究生,研究方向为隐私保护;荆长强(1985-),男,博士,副教授,研究方向为物联网应用;通讯作者:郭锋(1979-),男,博士,副教授,研究方向为工业物联网安全;武传坤(1967-),男,博士,教授,研究方向为密码学、物联网安全。

益和防止数据泄露等恶意攻击,隐私保护成为了至关重要的优先事项。在耗材管理系统中,不仅仅是耗材数据的隐私,还包括了用户数据的隐私,恶意的攻击者可以从服务器中获取耗材数据和用户数据来盗取隐私造成危害。如何保证数据在服务器中的安全以及能够查询则是一个不可忽视的问题,最传统的解决方法是将数据加密上传到服务器中,则在用户需要时将密文下载进行查询,这种方法在数据量比较大的情况下不适用,会消耗过多的内存[3]。另一种解决方法则是实现在服务器上密文匹配返回用户想要查询的数据。

随着隐私保护技术的不断进步,可搜索对称加密方案(Searchable Symmetric Encryption, SSE)应运而生,旨在解决先前提到的问题。该文提出一种面向耗材数据的简单实用且安全高效的可搜索对称加密方案,基于可搜索对称加密技术,结合哈希函数、AES 加密算法和伪随机函数原理[4]。方案采用对称加密算法对数据进行保护,并引入倒排索引结构以加速加密索引构建和查询搜索。不仅能够有效保护数据隐私,还能提高搜索效率和数据更新的便捷性。

1 相关工作

随着隐私保护问题的不断产生,可搜索对称加密被提出后已成为研究的热点,可搜索对称加密的研究也层出不穷。其技术的核心思想是用户在本地建立关键字与密文的索引,然后将这些索引与密文一起发送到服务器。当用户需要搜索时,它会生成与搜索关键字相对应的陷门将这些陷门发送给服务器。服务器根据用户发送的陷门进行搜索算法,然后将对应的加密文件返回给用户,最后进行解密得到明文[5]。

Song 等人[6]提出的第一个可搜索对称加密方案解决加密数据搜索,并提供安全性证明。但随文档的增多,搜索时间随之增长。服务器需逐字检查文档,导致搜索复杂度随文档增加线性上升,处理大型文档时性能下降。为了提高搜索效率,Curtmola 等人[7]提出一种基于倒排索引结构的可搜索对称加密方案,引入地址链的思想实现时间效率,指出以往安全模型存在的问题。Kamara 等人[8]提出了基于可搜索对称加密的动态方案,引入了删除矩阵作为索引构建的组成部分。每一对关键词和文档在索引结构中都会指向相应的删除矩阵。但删除操作通常只涉及文档一小部分,重新构建整个矩阵带来大的存储开销,代价高昂。Du 等人[9]提出基于倒排索引的可验证混淆关键字密文检索方案,为抵抗关键字攻击,利用 Paillier 技术对混淆关键字的搜索结果进行盲计算,减少通信开销,然而倒排索引的长度因关键字而异可能会引发数据攻击的风险。Li 等人[10]提出了一种基于伪随机函数的可搜索加密方案,旨在保护用户数据的隐私性。该方案简单易用、高空间复杂度且信息泄露少,同时易于更新。为数据隐私保护提供了有效且可行的解决方案。该方案使用的是直接索引的方式,在大量数据的情况下密文搜索时间也会逐渐变长。Zheng 等人[11]提出一种轻量级可搜索对称加密方案,通过分类存储和隐藏结构实现密文检索,但是在索引生成和密文检索效率上不够快。Zhu 等人[12]提出了两种边缘计算的新的可搜索加密方案,实现索引与陷门的精确匹配且空间复杂度低,并支持多关键字模糊查询,以致效率会减慢。Xiong 等人[13]提出了新的可搜索对称加密方案,利用布隆过滤器和改变索引结构方法,提高了搜索效率并解决了假阳性问题,同时对数据 ID 加盐增加安全性,但该方案需要对整个索引和 ID 遍历和匹配且具有额外的存储开销。Gao 等人[14]提出一种结合区块链和可搜索加密技术的方案,设计了动态倒排索引结构以完成密文搜索,倒排索引的字典形式存储结构可以使数据搜索时快速定位到包含关键字的文档,但在安全分析上不够,效率也有待进一步提高。为了保障耗材使用过程中用户数据的隐私,并确保系统具有高效的搜索功能,文中方案通过引入哈希算法和加密算法提高安全性,构建倒排索引提高密文搜索效率。

2 系统模型设计

2.1 威胁模型假设

在威胁模型中,文中方案假设服务器是一种诚实而好奇的攻击者类型。服务器具有完全的技术能力和访问权限,可以为用户提供正常的服务,类似于现有许多可搜索加密方案。尽管服务器具有良好的诚实特性,但也会出于好奇心对上传的数据进行分析或学习,以更深入地了解数据的内容,正如文献[15]所研究的内容。这种威胁模型充分考虑了服务器可能会尝试研究数据的情况,而不会破坏其正常服务功能。因此,文中方案需要在这种情况下保证数据的隐私,确保用户上传的数据不会被服务器用于其他目的。

2.2 系统模型设计

文中方案的系统模型主要包含两个参与者:用户和服务器。用户拥有原始的明文数据,并且会不断更新数据。系统模型的具体流程如图 1 所示。

首先,用户对明文数据进行加密索引的构建。该方案使用倒排索引的结构进行加密索引的构建。倒排索引是通过记录关键字出现的文档及位置来加速搜索的技术,该结构不仅用于明文的索引,还可以用于加密后数据的索引。用户在进行密文搜索时,即可通过倒排索引快速定位到包含关键字的加密数据集合。倒排索引结构具体如图 2 所示。

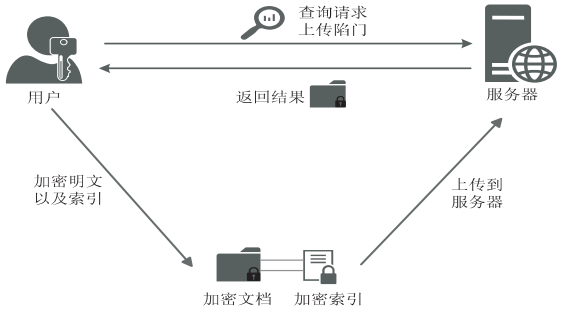

图 1　系统模型

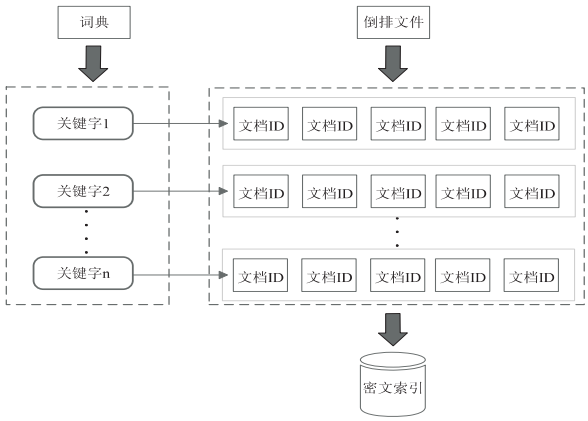

图 2　倒排索引结构

具体来说,该方案设计是通过字典形式存储关键字及对应文档列表,文档列表记录关键字在文档中的位置信息,这结构使搜索引擎能快速定位包含关键字的文档,实现高效信息搜索,效果不低于文献[16]。接着,参考文献[17]的流程,用户对明文数据进行常规加密算法加密,并将加密索引和密文一起上传到服务器中进行存储。服务器负责对数据进行存储和提供查询服务。当用户要查询某个数据时,用户输入关键字,关键字被加密成陷门后发送给服务器。服务器收到由关键字加密后生成的陷门,搜索匹配正确的索引,然后返回计算结果。为简化方案,仅考虑单个关键字的查询情况。

3　方案设计

3.1　方案概述

针对耗材数据上传到服务器存放过程中可能存在的用户数据隐私泄露和搜索效率低下等问题,该文提出了一种面向耗材数据的简单实用且安全高效的可搜索对称加密方案。该方案采用 KECCAK256 哈希算法和 AES 加密算法对数据进行处理。KECCAK256 是一种安全的哈希算法,能够将任意长度的消息哈希为固定长度的 256 位(32 字节)哈希值,这种算法具有高度的抗碰撞性和安全性。而 AES 加密算法是一种对称密钥加密算法,可以保证耗材数据的安全性,而且是被广泛认可和应用的加密标准,因此使用 AES 作为伪随机函数。伪随机函数(Pseudo-Random Function,PRF)的形式化定义[18]如下:

$$F:\{0,1\}^{k}\times\{0,1\}^{\text{in}}\rightarrow\{0,1\}^{\text{out}}$$

其中输入为密钥空间 × 输入空间。一个伪随机函数是安全的,因为伪随机函数 F 和真正的随机函数在计算上是不可区分的。对于任何给定的输入,伪随机函数生成的输出可能像是从真正随机函数里面获得的。其次敌手无法通过已知的 n 个对 $(x_i,F(x_i,k))$ 来预测下一个对 $(x_{(n+1)},F(x_{(n+1)},k))$,$k$ 为伪随机函数的输入密钥。这表明伪随机函数的输出对于敌手来说不可预测,可以认为伪随机函数是安全的[13]。

3.2　方案流程

文中方案的形式化定义包括如下算法[19]。其中 $D=\{D_1,D_2,\cdots,D_N\}$ 是明文数据集,N 是明文数据集中的数据量。

(1) KeyGen(k):客户端运行 KeyGen(k) 生成密钥 $\text{sk}\leftarrow\{0,1\}^{k}$,其中 k 为系统密钥。

(2) BuildInvertIndex(sk,D):该算法可以生成密文索引,客户端使用密钥 sk 和明文数据集 D,运行 BuildInvertIndex 生成密文索引 I。

(3) Trapdoor(sk,w):客户端使用密钥 sk 和关键字 w 运行 Trapdoor 生成陷门 T_w,得到对应的陷门 T_w。

(4) Search(I,T_w):服务器根据收到的加密索引 I 和陷门 T_w 运行 Search 算法,输出包含 T_w 的加密数据集合 $D(w)$。

在大部分的可搜索对称加密方案中是有框架要求的。在这个框架中,服务器保存加密后的文档和倒排索引,客户端负责生成和发送陷门 T_w 以及接收和解密搜索结果。通过使用哈希函数 h 和伪随机函数 F,客户端可以在不暴露明文关键字的情况下进行有效的搜索。同时,只有持有陷门 T_w 生成的密钥 sk 的客户端才能够生成正确的陷门 T_w,从而保证了安全性。该文设计的方案也遵守这一框架要求。具体包括如下几个不同的阶段。

(1) 在构建加密索引阶段,用户将需要运行 BuildInvertIndex(sk,D) 函数生成加密索引 I。用户需要对于数据 D_i 中的所有数据单元 $w_{i,j}(0\leqslant j\leqslant m)$ 进行遍历,计算哈希值 $h(w_{i,j})$。其中 $h:\{0,1\}^{*}\rightarrow\{0,1\}^{r}$ 是一个哈希函数,是将任意长度的比特串哈希到一个固定的 r 比特串,$w_{i,j}$ 是第 j 个数据单元中的第 i 块数据为 $(1\leqslant i\leqslant N,1\leqslant j\leqslant m)$,$m$ 是待检索的关键字数量。其次用户使用由 KeyGen(k) 生成的会话密钥 sk 对哈希值 $h(w_{i,j})$ 进行加密,生成 $T_{w_{i,j}}=F(\text{sk},h(w_{i,j}))$。$F:\{0,1\}^{k}\times\{0,1\}^{r}\rightarrow\{0,1\}^{r}$ 是一个伪随机函数,是用 k 比特密钥将一个 r 比特串映射到另一个 r 比特串,例如 F 可以用 AES 来实现。当加密完成后将数据单元 $w_{i,j}$ 以及对应的文档位置信息以图 2 的形式

进行存放,在存放的过程中会进行一次乱序操作,最终生成加密索引 I 并发送给服务器。

(2)在构建陷门阶段,用户输入待查询的关键字 w ,运行 Trapdoor(sk,w) 函数,使用密钥 sk 为关键字 w 计算陷门 $T_w = F(\mathrm{sk}, h(w))$,并将陷门 T_w 发送给服务器。

(3)在检索阶段,服务器接收到陷门 T_w 后,运行 Search(I,T_w) 函数对每一条加密索引进行计算和匹配,如匹配正确,返回陷门 T_w 对应的位置信息。

文中方案利用哈希函数、加密算法、伪随机函数以及基于倒排索引的结构,实现了加密索引的构建和检索过程。用户在构建索引时有效地保护了数据的隐私,查询时也不需要暴露关键字的明文。服务器在接收到陷门后能够进行具有安全性的检索操作,实现密文检索。该方案不仅高效,而且具有安全性。在数据更新过程中,只需将新的索引添加到原有索引中,无需修改原有索引结构。这种设计简化了更新操作,同时保持了系统的高效性和安全性。方案流程如图 3 所示。

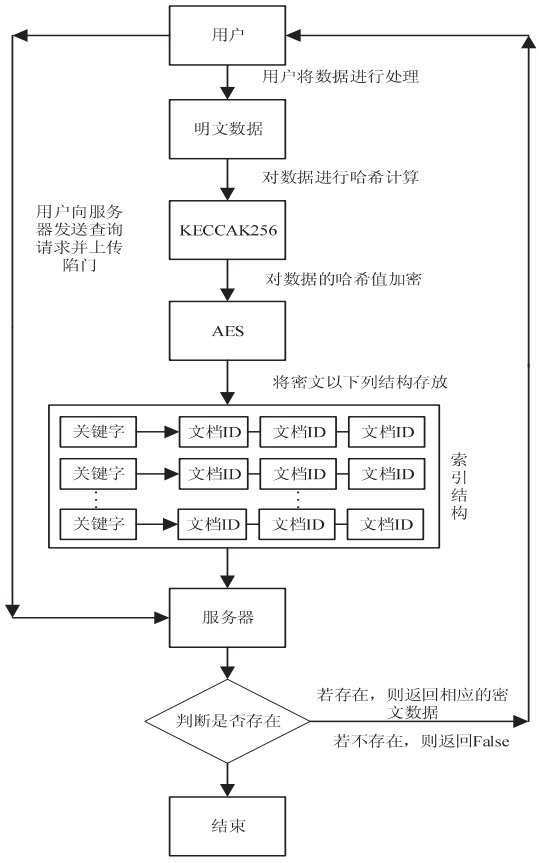

图 3 方案流程

4 实验验证和性能分析

4.1 实验环境与工具

实验环境如下:硬件设备为 Intel(R) Core(TM) i9-12900H CPU @ 2.50 GHz,并配备了 CUDA Toolkit 12.3 作为显卡。操作系统选择了 Windows 11。开发工具方面,使用了 pycharm 和 python3.8。在算法支持方面,采用了 pyCryptodome 密码算法库[20]提供的加密算法。pyCryptodome 密码算法库是基于 C 实现的,具有较快的密码学计算速度,尤其适用于处理大量数据或对性能要求较高的应用程序。文中方案主要使用了 KECCAK256 算法和 AES 算法作为加密算法。实验数据方面,使用了耗材管理系统中的真实数据。

4.2 正确性分析

为证明方案的正确性,主要从加密索引生成、陷门生成、匹配和搜索结果三部分进行分析[18]。

加密索引生成的正确性。对每个数据单元 $w_{i,j}$,先计算 $h(w_{i,j})$,使用密钥 sk 和伪随机函数 F 计算索引 $T_{w_{i,j}} = F(\mathrm{sk}, h(w_{i,j}))$ 。加密索引 I 包含所有加密的 $T_{w_{i,j}}$ 和对应的文档位置信息,并对其进行顺序打乱存储 $I = \{(T_{w_{i,j}}, \mathrm{pos}(w_{i,j}))\}$ 。

陷门生成的正确性。用户输入关键字 w ,计算 $h(w)$,使用密钥 sk 和伪随机函数 F 生成陷门 $T_w = F(\mathrm{sk}, h(w))$ 。

搜索匹配的正确性。服务器接收到陷门 T_w ,遍历加密索引 I ,计算并匹配若 $T_w = T_{w_{i,j}}$,则返回 $w_{i,j}$ 的位置信息。服务器返回匹配到的密文数据集合 $D(w) = \{D_i \mid \exists j, F(\mathrm{sk}, h(w)) = F(\mathrm{sk}, h(w_{i,j}))\}$ 。

4.3 服务器安全分析

在服务器内存储了密文以及加密索引两个方面。密文文件采用了 AES 加密算法对其进行加密处理,能够保证数据的安全性并且抵御选择明文攻击,索引也经过了多重加密处理[21]。首先使用哈希函数进行计算得到哈希值,然后对哈希值进行加密处理,最终以倒排文件的形式存放。在倒排文件中,加密的关键字和对应的地址是以顺序存放的,这可能给攻击者带来攻击机会。为了增加安全性,文中方案在存储倒排文件时将加密关键字和对应的地址一同乱序操作,这样攻击者无法从倒排文件的有序信息中获取关键字的顺序关系。这种处理方式可以有效地防止攻击者利用顺序信息进行攻击。文中方案也考虑到了索引的安全性,即使攻击者能够访问到加密索引,也无法直接从索引中推导出原始的明文内容或者与明文内容建立直接的关联。这是因为文中方案使用了哈希函数和伪随机函数来计算关键字,攻击者除非成功破解伪随机函数,否则无法从中获取有意义的信息。此外,哈希函数具有不可逆的特性,攻击者无法逆向推导出原始的明文。

4.4 用户安全分析

用户在进行查询时,向服务器发送的是加密关键字也就是陷门,这样的设计保证了用户在查询过程中使用的关键字不会被服务器获取到。当服务器匹配到

相应的结果后,并不会直接将明文返回给用户,而是以密文的形式进行返回[21]。通过这种方式,整个搜索过程中用户的隐私得到了有效的保护。

4.5　方案抵抗猜测攻击安全性分析

为了验证方案的安全性,该文将 KECCAK256 算法和 MD5 算法进行对比。KECCAK256 算法相较于 MD5 算法具有更强的防猜测攻击能力。猜测攻击是指攻击者根据关键字出现的频率和数量可能进行的攻击,尤其是在系统进行密文搜索时[22]。为了验证 KECCAK256 算法和 MD5 算法在防猜测攻击方面的安全性,在实验中对两者进行了比较。实验结果显示,使用 KECCAK256 算法和 MD5 算法的防猜测攻击能力的对比如图 4 所示。通过这些实验,可以展示 KECCAK256 相对于 MD5 在防范猜测攻击方面的优势。

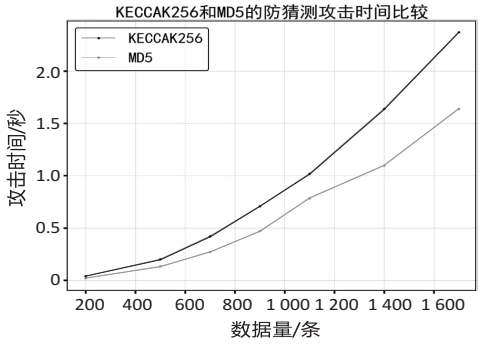

图 4　防猜测攻击时间的比较

在折线图中,纵坐标代表着服务器进行防猜测攻击所需的时间,而横坐标则表示数据量的大小。攻击时间越长,说明服务器需要花费越多的时间来进行防猜测攻击。在折线图中,不同哈希函数对应的线条位置越高,意味着在相同的数据量下,该哈希函数的防猜测攻击性能越差,需要越长的时间来完成攻击。因此,从图中可以清楚地看出 KECCAK256 算法在防猜测攻击方面表现出色,而相比之下,MD5 算法的性能相对较差。通过这些结果,得以验证 KECCAK256 算法在防范猜测攻击方面的优势。

4.6　方案的效率分析

为了验证方案的搜索有效性,与文献[12-13]提出的方案进行对比实验。在对比实验中,将从索引构建时间和服务器检索时间进行比较分析。

在整个方案中,时间消耗主要可以分为三部分:构建索引时间、构建陷门时间和服务器搜索时间。首先,构建索引和陷门的时间因为使用了哈希函数和伪随机函数,这些操作是必不可少的且需要计算时间。此外,由于索引的构建引入了新的存储形式,因此时间上可能会有所变化,需要进行实验验证。构建陷门只需要进行哈希和加密这些必要的操作,因此在这里不作详细讨论验证。此外,更加直观和关键的是服务器搜索时间,服务器搜索时间直接影响用户体验和搜索效率。

为了保证研究结果的准确性和可信度,该文对每个数据点进行了五次重复测试,并取平均值。通过折线图,比较了三种方案在不同数据量下构建索引和搜索的时间效率。从图 5 中可以观察到,文中方案在构建索引方面表现出较短的时间,这是因为采用了倒排索引结构,只需要对文档进行一次遍历。相比,文献[10,13]需要将整个文档内容以及 ID 都存储在索引中,从而增加了构建索引的时间和空间复杂度。而从图 6 中可以看出,文中方案比其余两个方案都快。这主要是由于倒排索引以字典形式存放,一旦获取到陷门,能直接定位到包含陷门的文档列表。文献[10]在查询时需要遍历索引,是具有线性复杂度的。文献[13]在使用布隆过滤器需要排除一些不匹配的情况,会消耗一定的时间。相比传统的线性扫描方法,倒排索引的搜索复杂度可以达到 $O(\log n)$ 级别,比线性扫描更适用于处理大规模数据集。这种结构极大地降低了搜索时间,提高了搜索效率。

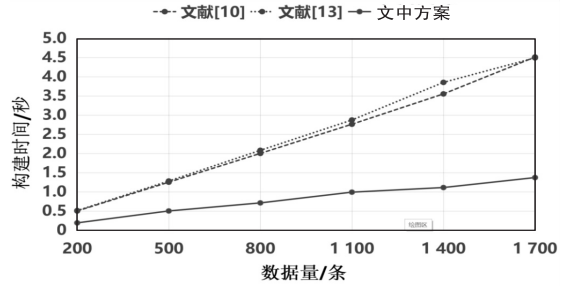

图 5　构建索引时间的比较

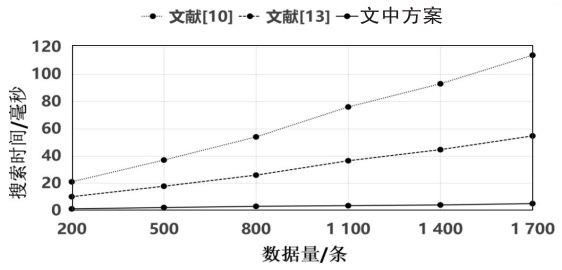

图 6　检索陷门时间的比较

下面是结构为倒排索引方案的搜索时间比较,文中方案仅对倒排索引结构的检索陷门时间进行了分析。通过图 7 可以看出,文中方案相较于文献[14,22-24]在检索陷门时间上的效率较高。

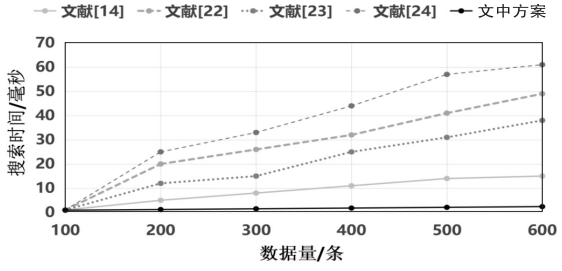

图 7　倒排索引方案的搜索时间比较

文中方案在构建索引和搜索时间上表现出了较高的效率和性能。通过倒排索引的简单结构和高效查询方式,文中方案能够在大数据量下保持较短的构建和搜索时间,为用户提供更快速高效的数据搜索服务。

5 结束语

针对耗材数据的特点提出了一种简单实用、安全高效的可搜索对称加密方案,有效解决了用户在使用耗材数据时的隐私问题。该方案主要针对单关键字搜索需求,并引入了倒排索引结构以提高密文检索效率。为了增强数据的安全性,该方案采用了 KECCAK256 算法和 AES 算法作为哈希函数和伪随机函数。这些算法的应用有效地加强了数据的保护,使得攻击者无法通过关键字获取明文信息。此外,在存储加密倒排索引时引入乱序操作,有效防止攻击者获取顺序关系分析索引文件从而推断出明文,进一步提升了数据的安全性。该方案使得用户能够在保障隐私的同时,高效地进行耗材数据的检索和查询,为数据的管理和利用提供了可靠的支持。但该方案也存在不足之处,在多关键字模糊查询方面尚未实现,以及可搜索加密方案的前向安全问题,进一步提高方案的安全性,这是未来需要解决的问题。

参考文献:

[1] YU Q,YANG W. The analysis and design of system of experimental consumables based on django and QR code[C]//2019 2nd international conference on safety produce informatization (IICSPI). Chongqing:IEEE,2019:137-141.

[2] YE Y. Design and implementation of an intelligent management system for consumables in open laboratory[C]//2021 4th international conference on advanced electronic materials,computers and software engineering (AEMCSE). Changsha:IEEE,2021:1342-1347.

[3] 孙国梓,王 钰,李兆维,等. 基于区块链的可搜索加密技术研究综述[J]. 南京邮电大学学报:自然科学版,2024,44(1):65-78.

[4] 王泽贤,汪学明. 一种改进的动态多用户前向安全可搜索加密方案[J]. 计算机应用与软件,2024,41(3):303-307.

[5] 王赟玲,陈晓峰. 对称可搜索加密技术研究进展[J]. 电子与信息学报,2020,42(10):2374-2385.

[6] SONG D X,WAGNER D,PERRIG A. Practical techniques for searches on encrypted data[C]//Proceeding 2000 IEEE symposium on security and privacy. California:IEEE,2000:44-55.

[7] CURTMOLA R,GARAY J,KAMARA S,et al. Searchable symmetric encryption: improved definitions and efficient constructions[C]//Proceedings of the 13th ACM conference on computer and communications security. Virginia:ACM,2006:79-88.

[8] KAMARA S,PAPAMANTHOU C,ROEDER T. Dynamic searchable symmetric encryption[C]//Proceedings of the 2012 ACM conference on computer and communications security. North Carolina:ACM,2012:965-976.

[9] 杜瑞忠,李明月,田俊峰,等. 基于倒排索引的可验证混淆关键字密文检索方案[J]. 软件学报,2019,30(8):2362-2374.

[10] LI J,NIU X,SUN J S. A practical searchable symmetric encryption scheme for smart grid data[C]//ICC 2019-2019 IEEE international conference on communications (ICC). Shanghai:IEEE,2019:1-6.

[11] 郑 东,王清瀚,秦宝东. 一种轻量级的对称可搜索加密方案[J]. 西安邮电大学学报,2020,25(3):1-6.

[12] ZHU J,WU T,LI J,et al. Multi-keyword cipher-text retrieval method for smart grid edge computing[J]. Journal of Physics:Conference Series. 2021,1754(1):012076.

[13] XIONG H. An efficient searchable symmetric encryption scheme for smart grid data[J]. Security and Communication Networks,2022,2022:9993963.

[14] 高改梅,王 娜,刘春霞,等. 基于区块链的可搜索加密电子病历共享方案[J/OL]. 计算机工程与应用,2024:1-12.

[15] 贾 强,张 帅,周福才. 一种面向密文大型数据集的可搜索加密方案[J]. 东北大学学报:自然科学版,2019,40(7):913-919.

[16] 孙晓玲,杨 光,沈焱萍,等. 基于可拆分倒排索引的可搜索加密方案[J]. 计算机应用,2021,41(11):3288-3294.

[17] 黄一才,李森森,郁 滨. 云环境下对称可搜索加密研究综述[J]. 电子与信息学报,2023,45(3):1134-1146.

[18] 许宗莲. 基于区块链的多用户动态可搜索对称加密方案研究[D]. 成都:电子科技大学,2022.

[19] 刘文心,高 莹. 对称可搜索加密的安全性研究进展[J]. 信息安全学报,2021,6(2):73-84.

[20] PASARELSKI R,ANGELOV K,POSTAGIAN K,et al. Implementation and analysis of a customized encryption algorithm in 5G networks for educational purposes[C]//2023 4th international conference on communications,information,electronic and energy systems (CIEES). Plovdiv: IEEE,2023:1-5.

[21] 王 莱,周腾达,王正飞,等. 基于布隆过滤器和 B+树构建倒排索引的电子病历密文搜索[J]. 计算机应用与软件,2021,38(4):276-280.

[22] 刘 炜,白晓丹,佘 维,等. 基于倒排索引的可搜索加密数据共享方案[J]. 计算机工程与应用,2023,59(10):270-279.

[23] 孙晓玲,杨 光,沈焱萍,等. 基于可拆分倒排索引的可搜索加密方案[J]. 计算机应用,2021,41(11):3288-3294.

[24] GE X,YU J,HU C,et al. Enabling efficient verifiable fuzzy keyword search over encrypted data in cloud computing[J]. IEEE Access,2018,6:45725-45739.