边缘计算模式下密文搜索与共享技术研究

王继锋[1,2]，王国峰[3]

（1. 西安交通大学管理学院，陕西 西安 710049；2. 国网汇通金财（北京）信息科技有限公司，北京 100053；
3. 朗新科技集团股份有限公司，江苏 无锡 214135）

摘 要：针对边缘计算数据安全问题，提出一种密文搜索与共享方案，在不改变边缘计算架构的和云计算架构的情况下，借助上述边缘计算诸多优势实现用户隐私数据保护，利用边缘节点构建加密倒排索引，在边缘节点和云计算平台之间安全地分享索引和密钥，实现密文搜索、数据安全共享及索引动态更新等功能。最后，与现有方案相比，对性能和安全性进行分析讨论，表明所提方案在密文搜索攻击模型下具有可证明的高安全强度，基于加密倒排索引兼顾了密文搜索效率和文档动态更新功能。

关键词：边缘计算；隐私保护；密文搜索；安全共享

中图分类号：TP302

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022039

Research on ciphertext search and sharing technology in edge computing mode

WANG Jifeng[1,2], WANG Guofeng[3]

1. School of Management, Xi'an Jiaotong University, Xi'an 710049, China
2. State Grid Huitong Jincai (Beijing) Information Technology Co., Ltd., Beijing 100053, China
3. LongShine Technology Group Co., Ltd., Wuxi 214135, China

Abstract: Aiming at the problem of edge computing data security, a ciphertext search and sharing solution was proposed, where the above-mentioned edge computing advantages were used to achieve user privacy data protection, edge nodes were used to construct encrypted inverted indexes, indexes and keys between edge nodes and cloud computing platforms were securely shared, and ciphertext search, secure data sharing, and dynamic index update were realized without changing the edge computing architecture and cloud computing architecture. Finally, compared to existing schemes, performance and security were analyzed and discussed, which proves that the proposed scheme has high security strength under ciphertext search attack model, and the ciphertext search efficiency and document dynamic update function are taken into account based on encrypted inverted index.

Keywords: edge computing, privacy protection, ciphertext search, secure sharing

0 引言

随着万物互联的高速发展，数据呈爆炸性趋势增长，物联网得到了快速发展[1]。2020 年，全球物联网设备数量达到 126 亿[2]，全球物联网市场规模达到 2 480 亿美元，预计到 2025 年全球物联网市场规模将超过 1.5 万亿美元[3]。随着 5G 通信、物联网等技术的快速发展，中国物联网市场规模由 2015 年的 7 510.6 亿元增长至 2019 年的 15 700 亿元[4]，且 2020 年中国新增 5G 连接设备超过 2 亿个，5G 基

收稿日期：2021−12−29；**修回日期**：2022−01−29

通信作者：王国峰，wangguofeng@bupt.cn

基金项目：国网电商公司（国网雄安金融科技集团）科技基金资助项目（No.19-JS-214）

Foundation Item: State Grid Electronic Commerce Co., Ltd. (State Grid Xiong'an Financial Technology Group Co., Ltd.) Foundation (No.19-JS-214)

础设施数量已跃居世界之首[5]。

万物互联时代，每天产生的数据量急增，数据在地理上分散，对数据安全性和响应时间都提出了更高的要求。云计算模式为大数据处理提供了高效的计算平台，但目前网络带宽的增长速度远远赶不上数据的增长速度[6-7]。因此需要解决带宽和时延两大瓶颈。边缘计算在靠近数据源头的网络边缘提供计算服务和存储资源，这里的边缘是指从云服务器到数据源之间的任意资源[6]。由于边缘计算能够在靠近终端设备的边缘节点处理和存储数据，从而能够较好地满足实时响应、多终端接入和节省网络流量等需求，受到学术界和工业界的高度关注[8]。

尽管边缘计算具有诸多优点，但也面临着各种隐私和安全威胁。作为云计算的拓展，边缘计算仍具有与云计算相同的数据安全问题：用户数据在云计算平台存储和计算，处于不可信环境中。针对此问题，用户的数据在上传至云计算平台之前，可利用近数据端的边缘节点直接对数据进行计算和处理，以保护用户隐私数据，降低边缘计算模式隐私泄露风险。由于边缘节点介于本地用户和云服务器之间，这一特性使在云计算模式中的典型的数据加密机制无法直接应用于边缘计算模式。因此，如何设计基于边缘计算的隐私数据保护和共享方案成为研究的热点和挑战。

本文利用边缘节点位于用户端这一优势，通过边缘节点对用户数据进行加密，保护用户隐私数据，将密文上传到云计算平台。然而，云计算平台难以对直接加密后的数据进行计算和数据搜索。本文针对此问题设计了边缘计算模式下密文搜索方案，使边缘节点与云计算平台协同配合，在边缘节点加密数据的同时，基于隐私保护数据构建加密索引，将密文索引上传到云计算平台，借助云计算平台实现密文搜索功能，在保护用户隐私数据的同时，提供对加密数据的搜索功能。

进一步地，不同用户的数据在不同边缘节点加密，密钥安全隔离，若数据上传者和数据使用者位于不同边缘节点下，如边缘节点 B 下的用户需要访问边缘节点 A 下的用户上传的数据，就需要在不同边缘节点之间进行数据安全共享。本文结合基于身份加密和公钥加密机制，实现密钥在不同边缘节点和云计算平台之间安全分享，从而实现数据隐私保护和安全共享。

由于边缘节点资源是动态变化的，需要密文搜索与共享方案能够根据业务和用户的动态需求，支持对文档内容进行动态更新，从而文档资源可按需调整，提升方案的灵活性；另外，如果位于边缘节点 A 下的用户移动到边缘节点 B 下，要在边缘节点 B 下搜索原来的数据，就需要对原来的密钥、索引和相关数据进行相应迁移。针对此问题，本文设计了一种数据动态更新方案，在边缘节点和云计算平台之间安全地同步和迁移索引，实现数据隐私保护和动态更新。

本文的主要贡献有以下几点。

1) 针对边缘计算模式设计安全性高、实用性好的密文搜索方案，并从查询性能和安全性方面对该方案进行系统的定量分析。从性能和安全性分析方面可以看出，本文设计的密文搜索方案安全性高，不需要专门定制及修改当前的云应用程序，是保护用户数据的有效解决方案。

2) 提出一种数据安全共享方案，结合身份加密和公钥加密，实现密钥在不同边缘节点和云计算平台之间安全分享，从而实现数据隐私保护和安全共享。

3) 设计加密索引动态更新方案，支持索引数据迁移同步，在添加、删除或更新文档内容时，依然支持用户进行数据搜索，使数据更新和数据搜索并行执行，从而提高事务执行效率。

1 相关工作

边缘计算在数据源头提供服务，将原有云计算中心的部分或全部任务迁移到边缘节点执行，使其在很多物联网应用和移动应用上发挥巨大作用，如增强现实、图像识别、网站性能优化、智慧城市、车联网等[7,9]。尽管边缘计算具有诸多优势，但也面临着数据隐私和安全威胁。本文假设边缘节点部署在用户侧，处于用户可控范围内，且是可信的；其他边缘节点和云计算平台部署在远端或云计算平台，处于半可信或恶意敌手的环境中。边缘节点介于本地用户和云计算平台之间，可以很好地过滤和保护用户数据隐私。

1.1 数据隐私保护

在用户数据传送到云计算平台之前，对数据加密可以有效保护用户的隐私数据。ShadowCrypt[10]利用浏览器插件对用户数据做加密保护，其针对的数据为文本型输入数据，不适用于更复杂的物联网场景。Mylar[11]针对 Web 应用服务防止用户隐私数据泄露，仅支持 Meteor JavaScript 框架，向后兼容

性不足。在边缘计算模式下，方晨等[12]基于区块链和联邦学习实现边缘计算隐私保护；巫光福等[13]基于区块链与云−边缘计算混合架构对车联网数据进行安全存储与共享；Kumari 等[14]基于 Carmichael 定理的改进同态加密方案保护医疗数据安全和隐私。

在保护用户数据隐私的前提下进行数据计算操作，可首先在本地对数据做特殊加密操作，然后在密文上进行计算。同态加密[15-17]和差分隐私[18-19]算法已广泛应用于此类场景。Lu 等[15]利用同态加密，为物联网异构设备设计了一种轻量级数据聚合方案，保护数据机密性和完整性，但没有涉及身份隐私和移动性。Lyu 等[20]设计了基于秘密共享和差分隐私的隐私保护数据聚合方案。该方案同样不涉及移动性。安全多方计算在多用户之间进行安全计算，同时保护各方输入数据的隐私[21-22]。很多文献使用混淆电路方法设计实际应用协议，如人脸识别[23]和远程诊断[24]，但这些方案需要很高的计算量及通信复杂度。基于秘密共享机制，Damgard 等[25]设计了一种用于相等性测试、比较和位分解的通用协议。为了提高效率，Nishide 等[26]构建了用于求解 2 个数大小关系的协议，不需要依赖位分解操作。Dinur 等[27]基于分布式离散对数问题设计了一个同态秘密共享协议。

1.2　密文数据搜索

针对密文数据搜索，Song 等[28]首先设计了一个可实用的方案，此方案搜索数据时需要云计算平台对密文数据进行全文扫描，具有一定的复杂度，安全性也需要进一步提高。Curtmola 等[29]构建倒排索引密文搜索方案，提高了安全性和搜索性能，但不支持文档动态更新。在边缘计算模式下，王娜等[30]基于分块技术设计了密文搜索方案；Li 等[31]利用云计算辅助设计了关键词排序搜索方案；Liu 等[32]设计了适合于边缘计算场景的数据安全搜索和存储方案。

为支持高级搜索功能，Kamara 等[33]通过维护复杂的数据结构设计密文搜索方案，实现动态更新机制。Boneh 等[34]构建关键字搜索公钥加密（PEKS, public key encryption with keyword search）算法实现多用户数据加密搜索，具有一定的时间开销。Liu 等[35]在 PEKS 基础上借助云计算平台参与计算，以提高计算性能。

1.3　密文安全共享

用户数据使用用户对应的密钥进行加密，密钥是私有的。如果某一用户 A 想要向另一用户 B 分享自己的某加密文档，用户 B 需要收到用户 A 的加密数据，同时需要从用户 A 获得密文数据对应的密钥，才能看到解密后的明文，所以加密密钥需要在不同用户之间安全地共享。

在边缘计算模式中，边缘节点可对用户数据进行加密，同时管理数据密钥。为实现不同边缘节点下的用户之间的数据共享，公钥加密（PKE, public key encryption）机制可有效地在不同边缘节点之间实现安全密钥共享。但 PKE 需确认身份证书的合法性，判断证书是否过期或撤销，产生很多证书状态查询请求，降低通信效率。身份加密（IBE, identity based encryption）机制可解决身份验证问题，但需要确保生成和托管私钥的计算节点是可信的。

Shamir[36]基于 IBE 提出一种加密和签名方案，但不具备可完全实用性。Boneh 等[37]基于 Weil 对设计了一种可实用的方案，但需要将私钥进行托管。为解决私钥托管问题，文献[38-39]利用 IBE 和 PKE 进行数据保护，Lewko 等[40]设计多授权方的数据加密方案。在边缘计算场景中，SHARE-ABE[41]基于属性加密方案设计数据共享框架；Zhang 等[42]在移动边缘计算模式中设计一种抗密钥滥用的轻量级数据共享方案。

为了安全地在边缘节点和云计算平台之间分享密钥，本文结合 IBE 和 PKE 设计密钥安全共享方案，利用云计算平台计算和存储能力，实现不同用户之间的密文共享机制。

2　密文搜索与共享系统模型

2.1　背景知识

令 $\{0,1\}^m$ 代表所有 m 位字符串的集合。$x \xleftarrow{R} X$ 为从分布 X 中随机取元素 x，$x \xleftarrow{R} S$ 为从集合 S 中随机取元素 x，$x \leftarrow A'$ 为经过算法 A' 得到 x。Z_q 为加法群 $\{0,1,\cdots,q-1\}$，q 为模。Z_q^* 为 Z_q 中去除单位元 O 的集合。对于足够大的 s 和任意多项式 $p(\cdot)$，若函数 f 满足 $f(s)<\dfrac{1}{p(s)}$，则认为 $f(s)$ 为可忽略的。给定任意概率多项式时间算法 A'，分布 X 和 Y 计算不可区分需满足

$$\left|\Pr\left[A'(X)=1\right]-\Pr\left[A'(Y)=1\right]\right|<\frac{1}{p(s)} \tag{1}$$

伪随机函数 f 的安全性满足 $\{0,1\}^m \times \{0,1\}^n \to \{0,1\}^s$，其是多项式时间可计算的，其中，$m,n,s>0$。对任意随机函数 F、概率多项式时间对手 A、足够大 s 和多项式 p，有

$$|\Pr[A^{f_k(\cdot)}=1:k\xleftarrow{R}\{0,1\}^s]-\Pr[A^{g(\cdot)}=1:g\xleftarrow{R}\{F:\{0,1\}^n\to\{0,1\}^m\}]|<\frac{1}{p(s)} \tag{2}$$

对称加密算法 E 安全性满足：对任意概率多项式时间对手 A、足够大 s 和多项式 p，有

$$\Pr[b'=b:k\leftarrow K(1^s);(m_0,m_1)\leftarrow A^{E_k(\cdot)\mathrm{De}_k(\cdot)};b\xleftarrow{R}\{0,1\};c\leftarrow E_k(m_b);b'\leftarrow A^{E_k(\cdot)\mathrm{De}_k(\cdot)}(c)]<\frac{1}{p(s)} \tag{3}$$

其中，A 得不到 c 的明文信息，$|m_0|=|m_1|$。若方案 $e=(K, E, \mathrm{De})$ 满足以上安全性，则具有选择密文攻击安全性，其中，K 表示密钥算法，E 表示加密算法，De 表示解密算法。

可搜索加密算法一般包含如下多项式时间算法。

1) 密钥生成算法。由安全参数 s 作为输入，生成密钥 k，k= KeyGen(s)。

2）索引生成算法。由文档集合 D 和密钥 k 作为输入，生成索引 I，I= BuildIndex(k,D)。

3) 令牌生成算法。由密钥 k 和关键字 w 作为输入，生成搜索令牌 T_w，T_w= Trapdoor(k,w)。

4) 搜索算法。由搜索令牌 T_w 和索引 I 作为输入，生成针对文档集合 D 的查询结果 $D(w)$，$D(w)$= Search(T_w,I)。

针对密文搜索的攻击主要有 2 个目标，一是猜测用户查询的关键字，即得到查询令牌和关键字的映射关系；二是猜测密文内容。

在密文搜索相关术语中，搜索模式是指对于返回结果相同的 2 个搜索令牌，能否决定这 2 个搜索令牌对应于同一个关键字的概率不大于 $\frac{1}{2}$。访问模式是指从返回结果中能够获取的信息，如判定 2 个文档同时含有的关键字的信息[43-44]。

密文搜索安全性级别定义如下。

选择明文攻击（CPA, chosen plaintext attack）安全性。在未查询前提下，密文及索引不会泄露有关明文的任何信息，但有可能泄露其他信息，如文档中关键字个数信息或位置信息。

非自适应选择关键字攻击（CKA1, non-adaptive chosen keyword attack）安全性。攻击者在一次查询的前提下，密文和索引除泄露搜索模式和访问模式以外不会泄露其他有关明文和关键字的信息。

自适应选择关键字攻击（CKA2, adaptive chosen keyword attack）安全性。允许攻击者在已搜索的令牌和搜索结果的基础上发出查询请求，密文和索引除泄露搜索模式和访问模式以外不会泄露其他有关明文和关键字的信息。

根据密文搜索泄露信息划分安全等级从低到高排列如下。

Le4：云计算平台可以得知关键字在文档中的具体位置和出现次数。

Le3：云计算平台可以得知哪些文档中含有相同的关键字，关键字在文档中第一次出现的位置（不知道具体每一次的位置和出现次数）。

Le2：云计算平台可以得知哪些文档中含有相同的关键字。

Le1：仅当用户使用查询功能时，云计算平台才能得知哪些文档中含有相同的关键字。随着用户查询次数逐渐增多，云计算平台得知的信息也逐渐积累，该安全模型逐渐退化为 Le2。

Le0：在 Le1 的基础上，即使多次查询也不暴露文档中含有相同的关键字的信息。仅会暴露常规查询统计信息（文档的密文长度、查询用户的 IP 地址和查询频率等）。

密文搜索的攻击者的前置知识等级及关联如图 1 所示。

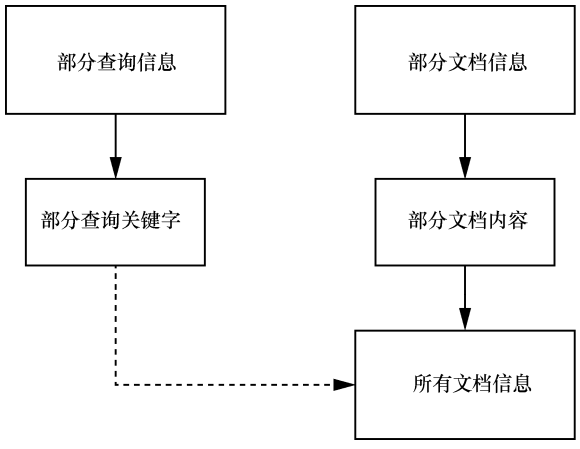

图 1 攻击者的前置知识等级及关联

预知查询信息。1) 部分查询信息：例如文档内容为微信聊天记录，攻击者可以参考典型用户的使用习惯，推测用户关心的内容和比较常用的关键字等。2) 部分查询关键字：攻击者知道某些确切

的查询关键字，即部分查询令牌和对应的关键字已泄露给了攻击者，攻击者试图猜测所有的查询关键字内容。

预知文档信息。1) 部分文档信息：例如文档为邮件内容，攻击者可以根据用户的身份大致知道邮件可能的类型，如财务报表、竞拍的标底、合同协议等。2) 部分文档内容：知道某些确切的文档内容或某些文档的重要信息，知道文档集合一定包含某些内容，例如群发邮件被攻击者获取等。3) 所有文档信息：不仅知道全部的明文文档内容，而且知道某些查询对应的确切关键字。

针对密文搜索的攻击者可分为 2 种。1) 被动攻击者：遵从正常的服务流程，不主动进行攻击，希望通过用户的查询猜测出“密文文档内容”和“查询关键字内容”。2) 主动攻击者：利用攻击或欺骗手段获取文档集合中的某些选定文档，或诱导用户进行某一选定的查询。根据密文搜索攻击相关文献[43-44]，攻击方法可通过对明文及密文搜索过程和结果进行统计，利用查询计数进行查询恢复攻击（即查询某关键字返回结果和对应文档个数），或根据关键字对或多个关键字在同一文档中共同出现的概率进行拟合和优化得到明文内容。

2.2　系统模型

边缘计算由多个位于本地设备和云计算平台之间的边缘节点协同完成数据存储与计算任务。一般而言，边缘节点与用户之间的链接和安全更可靠，与云计算平台之间的交互和链接更稳定。如在边缘节点就是用户的主机上的虚拟机或局域网服务器的场景下，用户可以将隐私信息直接发送给边缘节点处理，边缘节点与用户之间的可信度很高。再如某公司某一业务上云，该业务由不同部门合作完成，各部门位于不同地区，相互之间存在数据交互。各部门分别在己方可信环境内部署边缘节点，用于和云计算平台及其他部门展开业务交互。这种情况下己方的边缘节点被认为是可信的，云计算平台和其他部门的边缘节点被认为是“诚实而好奇”的半可信实体，己方部门用户的数据隐私安全问题需要受到保护。

边缘计算模式下密文搜索与共享系统架构由用户、边缘节点和云计算平台 3 个关键角色组成，如图 2 所示，利用边缘节点位置和功能的特殊性，对用户和云计算平台之间的传输数据进行加密和索引，以保护用户的隐私数据，并实现搜索功能；同时利用云计算平台超强计算能力和超大存储空间，存储密文数据并维护和更新数据索引。用户数据在边缘节点处进行加密，构建索引，同时密文数据和加密索引同步更新到云计算平台。当用户检索数据时，密文搜索功能由云计算平台执行，由云计算平台返回相应的密文数据。如果返回的密文在边缘节点处有对应的密钥，则可直接解密返回给用户；如果没有对应的密钥，则需要和密钥所在的边缘节点进行密钥安全传输，获得相应的密钥后即可对密文进行解密。当用户对原始文件数据修改后，对应的文件索引需要同步更新，以确保正确的检索结果。

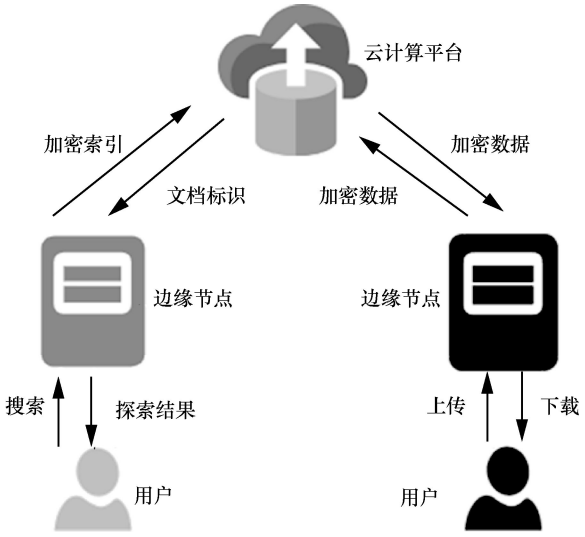

图 2　密文搜索与共享系统架构

在密文搜索与共享系统架构中，边缘节点隐私保护机制通过识别和过滤应用层协议来加密和保护用户的隐私数据。隐私数据保护主要由以下功能模块组成。

1) 数据识别模块。根据服务器名称标识（SNI, server name indication）、统一资源定位符（URL, uniform resource locator）等特征字段分析应用协议，识别用户隐私数据。通过分析请求内容格式，找到要加密的数据，以交给数据加密模块加密明文数据；并把要搜索的数据交给索引服务模块构建索引。

2) 数据加密模块。加解密用户隐私数据，针对属于同一文件的用户数据，构造密文元数据。元数据内容包括密钥标识、边缘节点标识、特征标识等。元数据存储在边缘节点处，用于标识加密数据，以便接收到密文数据时，可以识别并找到对应的密钥进行解密。解密操作根据元数据中的特征标识定位到密文内容，利用密钥标识获得密钥并解密。

3) 索引服务模块。当用户加密后的文件上传到云计算平台后，会返回对应的文件标识符。索引服务模块得到文件标识符和数据识别模块缓存的明文数据并建立加密索引，在文件数据更新时维护和更新搜索索引。边缘节点建立的索引同步更新到云计算平台，由云计算平台融合和管理各边缘节点上传的索引数据，形成统一的搜索索引，成为主索引。当用户文件更新后，边缘节点形成索引更新数据，并上传到云计算平台，由云计算平台在主索引上完成同步更新。典型步骤执行过程如下。

首先，数据识别模块处理用户数据，识别并缓存要加密的隐私数据。然后，数据加密模块生成密钥加密数据，将元数据附到密文头部，并在数据库中存放密钥和密钥标识；边缘节点将加密后的文件数据发送到云计算平台后，接收返回的文件标识符。最后，索引服务模块使用缓存的文件数据和文件标识符建立索引，并将索引及时与云计算平台同步。

当加密数据由云计算平台返回后，数据加密模块通过分析特征标识定位密文数据；根据密文头部元数据中的密钥标识获得对应密钥并解密，将明文数据返回给用户。

当用户输入查询内容进行搜索操作时，边缘节点根据查询请求获得要搜索的关键字，然后向云计算平台发起检索请求。云计算平台根据检索请求返回对应的文件标识符，用户利用文件标识符请求对应的密文文档，当云计算平台返回相对应的密文文档后，边缘节点获取密文文档对应的密钥，解密并将明文数据返回给用户。

3 密文搜索与共享技术方案

边缘计算模式下密文搜索与共享技术利用边缘节点对用户数据加密，将密文上传到云计算平台上，需要针对密文数据实现搜索、共享和动态更新等功能。本文针对此问题分别设计密文搜索、数据安全共享及索引动态更新机制，使边缘节点与云计算平台协同配合，在边缘节点加密数据的同时，基于隐私保护数据构建加密索引，借助云计算平台实现密文搜索功能，同时实现索引数据同步和动态更新方案，结合 IBE 和 PKE 实现密钥安全共享，在保护用户隐私数据的同时，提供对加密数据的搜索、共享和动态更新功能。

3.1 密文搜索方案

在边缘节点处加密数据势必与云计算平台的数据计算功能产生冲突，如数据搜索功能。针对此问题，本文设计了基于加密索引的密文搜索方案，在保护用户隐私数据的同时，提供对加密数据的搜索功能。

基于加密索引的密文搜索方案在云计算平台执行搜索和更新操作，搜索过程不泄露明文信息，只泄露一定的搜索模式和访问模式。在边缘节点处，每个关键字 w 被确定性加密成可搜索的令牌 $f(w)$，并对应建立由 $|D(w)|+\Omega$ 个文档节点组成的倒排列表，其中，D 表示文档集合，$|D(w)|$表示文档集合 D 中含有关键字 w 的文档的个数，Ω 表示填充节点个数。每个文档节点包含两部分，一部分是被加密的含有 w 的密文文档的标识符，另一部分是指向下一个文档节点的指针。文档节点以随机顺序排列。

密文搜索索引结构如图 3 所示，对于关键字 K，经确定性加密映射 f 得到令牌 T，建立倒排列表 $L(T)$，长度为 $|D(w)|+\Omega$，Ω 表示填充节点 Δ 的个数，根据含有关键字的文档个数调整 Ω 的大小，使每个关键字的倒排列表含有的节点个数一致。$L(T)$的每个节点包含含有关键字 K 的文档 D_i 的加密文档

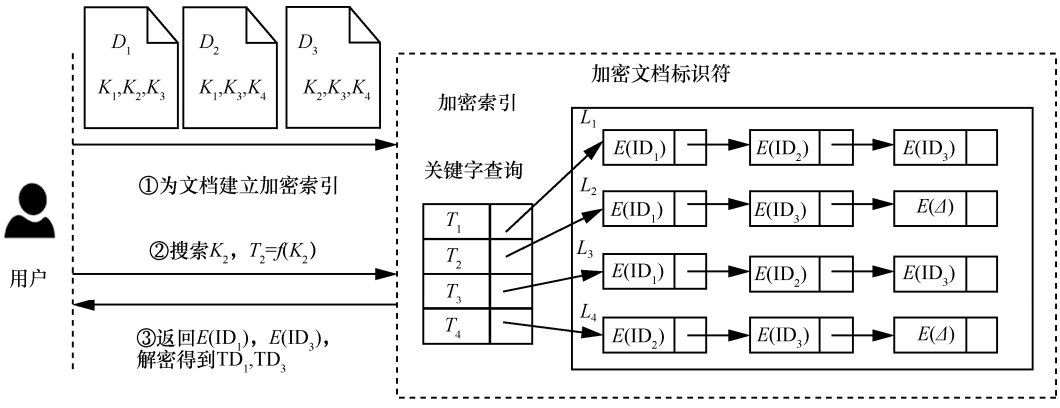

图 3 密文搜索索引结构

标识符，以及指向下一个节点的指针。给定关键字 K，通过 f 得到令牌 T，获得对应的倒排列表。

基于加密索引的密文搜索方案索引建立过程如下。

1) 边缘节点从文档中提取不同关键字，对关键字通过确定性加密 f 得到可搜索令牌 T。

2) 边缘节点将令牌和相应的密文文档标识符做映射并索引，并上传加密索引到云计算平台。

3) 遇到搜索请求时，边缘节点首先解析关键字，得到对应的令牌，并发送给云计算平台，由云计算平台执行搜索操作，返回密文文档标识符结果。

在边缘计算场景下，边缘节点解密得到的密文文档标识符搜索结果后，根据用户需求，把需要得到数据内容的文档标识符发送给云计算平台。当接收到加密文档数据后，边缘节点解密相关文档得到明文内容。在搜索过程中文档标识符是加密的，从而无法利用查询结果推断关键字共现频率，一定程度上隐藏了访问模式。

根据加密算法 E 和确定性加密 f 的安全性定义，除文档和索引大小信息之外，索引数据结构没有泄露其他信息，在搜索过程中除了一定的搜索模式和访问模式信息之外没有泄露其他任何信息。在实际搜索场景中，用户对搜索到的文档标识符结果列表，通常会针对部分感兴趣的文档进行查看，发起文档内容获取请求。由于搜索结果列表和具体文档内容获取请求没有固定的对应关系，云计算平台无法确定某一搜索请求的确定性结果，从而一定程度上隐藏了搜索的访问模式。

3.2　数据安全共享

用户数据在边缘节点处加密，即相应的密钥存储在边缘节点中。在不同边缘节点之间共享密文数据，需要解决如何在不同边缘节点之间安全地分享用于解密数据的密钥的问题。

PKE 公钥加密方案可确保加密密钥在不同边缘节点间安全共享。但在 PKE 方案中，为验证身份有效性，需要执行大量验证证书合法性的操作。本文结合 IBE 和 PKE 实现数据安全共享方案，采用 PKE 方案[45]保证密钥的安全传输，利用基于身份的加密 IBE 方案[37]解决证书验证问题，确保密钥在边缘节点之间安全传输。

数据安全共享方案使用控制节点充当 IBE 方案的 PKG。这里控制节点可以在云计算平台设置，也可以由第三方机构代理。密钥传输有 PKE 加密层保护，即使控制节点是不可信的，由于其没有 PKE 私钥，故无法获取明文内容。边缘节点使用 PKE 公钥−私钥对及身份 ID 和控制节点进行交互，完成身份验证。通过验证，控制节点签发 ID 对应的 IBE 私钥。令 PK_I 代表 IBE 公钥，SK_I 代表 IBE 私钥，PK_P 代表 PKE 公钥，SK_P 代表 PKE 私钥，id(C)代表密文 C 的元数据。如图 4 所示，加密密钥在不同边缘节点之间传输过程如下。

1) 边缘节点 B 从云计算平台接收到密文数据，将密文元数据发送到控制节点。

2) 控制节点根据密文元数据中的边缘节点标识得到对应的边缘节点 A，从 A 处请求解密密钥。请求携带的参数包括密钥标识、边缘节点 B 的时间参数 t_B、B 的身份标识 ID_B、B 的 PKE 公钥 $PK_{P\text{-}B}$。时间参数 t 可用来更新边缘节点对应的 IBE 私钥，以提高加密安全性。

3) A 收到请求，根据 t_B、ID_B 参数得到 $PK_{I\text{-}B}$，利用 $PK_{P\text{-}B}$ 对密钥做双重加密，并将加密后的密钥发送给 B。

4) B 接收到消息后，使用 $SK_{I\text{-}B}$ 和 $SK_{P\text{-}B}$ 解密获得数据密钥，即可获得对应的明文数据。

在上述方案中，密钥生成、参数选择和加解密过程等均遵循标准 IBE 方案[37]和 PKE 方案[45]，密钥被 PKE 公钥和 IBE 公钥双层加密。控制节点获取不到边缘节点的 PKE 私钥，故无法窃取密钥。即使某攻击者获得了 PKE 私钥，如果没有 IBE 私钥，也无法解密获得密钥。边缘节点同时具有与 ID 对应的 IBE 私钥和 PKE 私钥，故数据安全共享方案确保了密钥被安全传输。

3.3　索引动态更新

基于加密索引的密文搜索方案支持数据动态更新，即可添加、删除文档或修改文档内容。在动态更新方案中，在云计算平台和各边缘节点处都维护着一份倒排索引结构，云计算平台为主索引，执行实际的搜索功能，并融合合并各边缘节点的临时辅助索引。索引动态更新如图 5 所示。

添加新文档时，边缘节点中的索引服务模块构建临时索引。删除文档时，边缘节点更新对应文档标识符的无效位向量，标识文档被删除，在返回检索结果前过滤已删除文档。若更新某文档，则将此文档删除并重新添加文档。执行更新索引结构操作后，边缘节点的索引服务器将辅助索引上传到云计

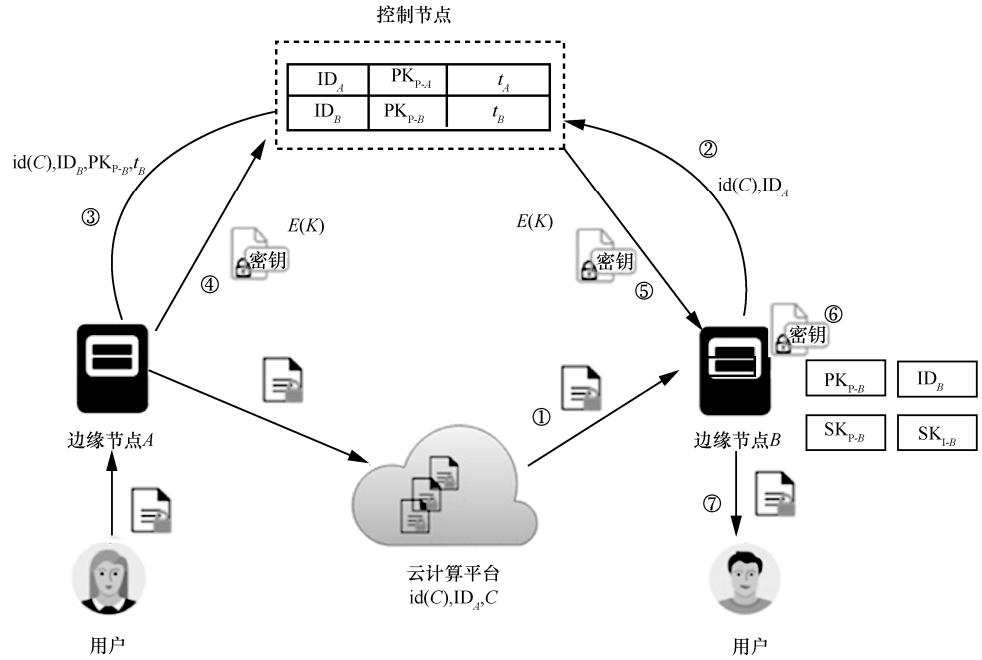

图 4　密钥分享架构

算平台，与主索引进行合并，将新文档节点插入对应的关键字令牌列表中，完成动态更新操作。

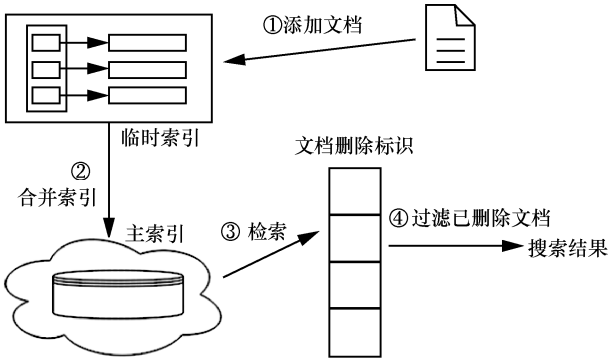

图 5　索引动态更新

为了索引更新和搜索并行计算，可以在云计算平台维护两份索引，一份执行搜索操作，另一份进行索引更新，更新完成后在两份索引之间执行数据同步操作。另外，边缘节点和云计算平台可以建立索引数据同步更新，在特殊情况下，搜索操作可以在边缘节点执行，从而向云计算平台隐藏了搜索行为。

为了提高数据传输效率并节省带宽，本文参考 Rsync 算法[46]和端云协同数据同步方案[47]，设计了数据迁移同步方案，包括数据迁移与数据同步更新，数据迁移同步过程具体如下。

1) 将源文件 $\boldsymbol{F}$ 切分成大小相同的 n 块，$\boldsymbol{F}=[f_1,f_2,\cdots,f_n]$。

2) 构造生成矩阵 **GM**（任意 $n\times n$ 子矩阵的秩为 n），上部分为 $n\times n$ 的单位矩阵，下部分为 $m\times n$ 的范德蒙德矩阵，m 为生成冗余块的个数。利用 **GM** 将 n 个文件块通过式(4)编码成 $n+m$ 个编码块 $\boldsymbol{C}$，$\boldsymbol{C}=[c_1,c_2,\cdots,c_n,\cdots,c_{n+m}]^{\mathrm{T}}$，则有

$$\boldsymbol{C}=\mathbf{GM}\cdot\boldsymbol{F}^{\mathrm{T}} \tag{4}$$

3) 得到编码块 $\boldsymbol{C}$ 后，随机选取 n 个线性无关的编码块 $\boldsymbol{C}_n$，利用 **GM** 可恢复成源文件 F，即

$$F=\mathbf{GM}^{-1}\boldsymbol{C}_n \tag{5}$$

由上述过程可知，即使传输过程中某一编码块丢失或损坏，也可通过生成矩阵 **GM** 和选取的 n 个线性无关的编码块 $\boldsymbol{C}_n$ 进行恢复。

在数据同步更新过程中，假设旧文件为 $\boldsymbol{F}^{v_1}=[f_1^{v_1},f_2^{v_1},\cdots,f_n^{v_1}]$，新文件为 $\boldsymbol{F}^{v_2}=[f_1^{v_2},f_2^{v_2},\cdots,f_n^{v_2}]$，具体步骤如下。

1) 计算差分文件 $\boldsymbol{\Delta}^{v_1,v_2}$，表示新文件 $\boldsymbol{F}^{v_2}$ 与旧文件 $\boldsymbol{F}^{v_1}$ 之间的差异，内容匹配位为 0，不匹配位为 1，即

$$\boldsymbol{\Delta}^{v_1,v_2}=\boldsymbol{F}^{v_2}-\boldsymbol{F}^{v_1}=[\delta_1^{(v_1,v_2)},\delta_2^{(v_1,v_2)},\cdots,\delta_n^{(v_1,v_2)}] \tag{6}$$

其中，$\delta_i^{v_1,v_2}=f_i^{v_2}-f_i^{v_1}$。

2) 通过生成矩阵 **GM** 和 $\boldsymbol{\Delta}^{v_1,v_2}$，得到差分文件编码块集合 $\boldsymbol{\Delta}_c^{v_1,v_2}$ 为

$$\boldsymbol{\Delta}_c^{v_1,v_2}=\mathbf{GM}\boldsymbol{\Delta}^{v_1,v_2}=[\delta_{c_1}^{v_1,v_2},\delta_{c_2}^{v_1,v_2},\cdots,\delta_{c_n}^{v_1,v_2},\cdots,\delta_{c_{n+m}}^{v_1,v_2}] \tag{7}$$

3) $\Delta_c^{v_1,v_2}$ 中很多编码块内的元素都取值为 0，产生变化的编码块集合记为 $\Delta_{nc}^{v_1,v_2}$。通过待更新文件编码块集合 $\boldsymbol{C}^{v_1}$ 计算新的文件编码块集合 $\boldsymbol{C}^{v_2}$。

$$\boldsymbol{C}^{v_2} = \boldsymbol{C}^{v_1} + \Delta_{nc}^{v_1,v_2} \tag{8}$$

4) 根据式(8)，利用 $\Delta_{nc}^{v_1,v_2}$ 可完成文件编码块的同步更新，同时完成新文件 $\boldsymbol{F}^{v_2}$ 和旧文件 $\boldsymbol{F}^{v_1}$ 之间的同步更新。

另外，可设置当新旧文件变化率 $\mathrm{CF}=\dfrac{\Delta^{v_1,v_2}}{\boldsymbol{F}^{v_1}}$ 大于某一阈值时才进行同步更新，否则延迟更新，从而减少资源浪费和通信带宽。

4　性能与安全性分析

本文搭建了一个原型系统来模拟边缘节点加密数据和解密数据的性能和安全性。所用虚拟机配置包括 2.5 GHz 双核英特尔处理器，2 GB 内存，上行速度约为 1 000 KB/s，下行速度约为 7 500 KB/s。边缘节点作为服务解析云计算平台和用户之间的数据连接，保护用户隐私数据。

为了测试数据加密和解密性能，借助 Gnu 隐私保护（GPG, Gnu privacy guard）加密工具，采用 AES256 加密算法，分别发送和接收如下类型的文件：32 KB 文本，107 KB 压缩文件，2 MB、31 MB、532 MB 可执行程序和 1.3 GB 压缩文件。从图 6 可以看出，边缘节点加密小文件消耗时间较少，加密大文件消耗时间较多。在实际应用场景中，大文件往往采取分块传输的方式，针对数据块加密并传输，故可以大大缩小加密大文件数据的时间。

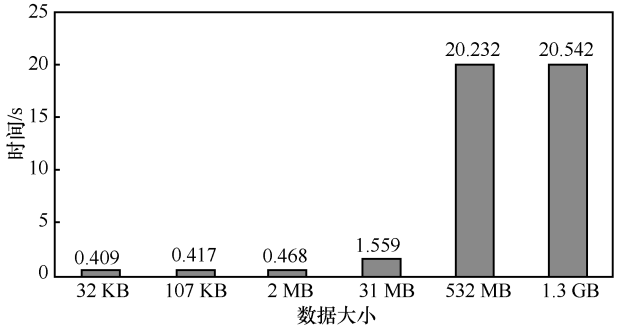

图 6　数据加密性能测试

图 7 展示了接收加密数据时，边缘节点解密操作带来的额外开销。从图 7 中可以看出，当文件数据块不大于 31 MB 时，边缘节点解密文件数据带来的额外开销较小。

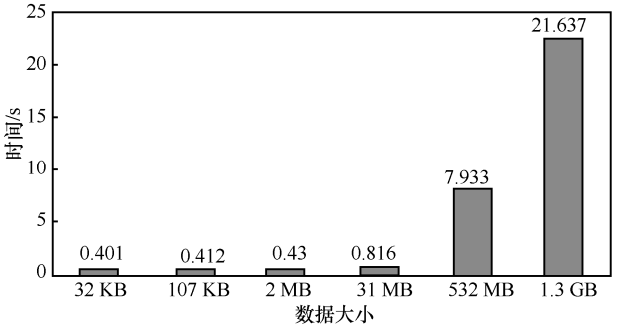

图 7　边缘节点解密操作带来的额外开销

本文密文搜索方案建立倒排索引进行搜索，实现最优查询效率，并可大大节省时间和空间消耗。令 m 为所有文档不同的关键字的个数，n 为文档数量，$R(w)$为搜索关键字 w 对应的含有此关键字的文档集合，E_t 为加密时间消耗，D_t 为解密时间消耗，a 为各文档含有的关键字个数的平均值，v 为各关键字对应的文档列表的平均长度，l 为各关键字对应的文档列表的最长的长度，各密文搜索方案相关功性能对比如表 1 所示。

表 1　　不同密文搜索方案功性能对比

方案	加密方式	是否索引	索引大小	搜索时间	动态更新	安全级别
文献[28]	哈希	非索引	非索引	anE_t	非索引	CPA
文献[29]	对称	倒排索引	$O(vm)$	$R(w)D_t$	不支持	CKA1
本文方案	对称	倒排索引	$O(lm)$	$R(w)D_t$+ΩD_t	支持	CKA2

从表 1 中可以看出，文献[28]对文档中关键字逐一进行伪随机函数加密生成可搜索密文，搜索时间与文档中关键字个数有关，泄露了文档中关键字个数和位置，属于 CPA 安全级别。文献[29]基于倒排索引构建密文搜索方案，与本文区别为其加密节点中指向下一加密节点的指针也被加密，不支持文档动态更新功能，需要将云计算平台密文下载到本地，重新构建索引后上传，在不考虑填充节点的情况下，其安全级别为 CKA1。本文密文搜索方案指向加密节点的指针未被加密，支持索引动态更新功能，索引构建大小与关键字对应的文档列表的最长长度有关，搜索时间复杂度与含有关键字的文档列表的长度及填充节点个数相关，安全级别为 CKA2。

令 N 表示文档更新一次变化的关键字的个数，动态更新方案添加文档时在边缘节点先建立临时索引，建好后同步到云计算平台，更新时间与 N 正相关，从

而大大减少了执行时间。删除文档时在边缘节点处建立含有文档标识的无效位向量，会消耗一定的内存，同时返回结果进行过滤会消耗一定的时间，可以考虑构建哈希映射数据结构，快速得到文档是否已被删除的结果。密文搜索方案在边缘节点处构建索引，同步到云计算平台，并在云计算平台执行搜索操作，具有很高的查询性能。本文方案在边缘节点处存储一定的数据，带来一定的空间开销。经 Rally 软件评估测试，对于 1.2 GB 大小的文件集合，构建的索引大小约为 0.9 GB，查询效率约为 19.6 ops/s。

在不同边缘节点分享密钥场景下，使用 GPG 库生成 4 096 位的 PKE 公私钥对，使用双线性密码（PBC, pairing based cryptography）库生成 IBE 双线性对。由于密钥数据很小，密钥双层加密和解密方案引入的开销很小，是毫秒级别的。

在安全性方面，本文假定用户侧边缘节点是可信和安全的，即数据在边缘节点中以明文形式传输。边缘节点之外的路径如云服务器或其他边缘节点是不可信的。敏感数据在传递到外部之前被边缘节点加密，加密数据上传到云计算平台，云计算平台无法获取位于边缘节点存储的相应密钥，得不到明文信息，从而有效防止了云计算平台窃取敏感数据。在边缘节点外部，即使用户账户信息泄露，攻击者也只能得到密文数据，因此本文方案可有效保护云服务中用户的隐私数据。

参考文献[29,33]，利用 Real/Ideal 模拟范式定义可搜索加密安全性，L 表示有状态的泄露函数，存在一个模拟器 S，以 $L(P)$为输入，P 表示历史协议；$S(L(P))$表示输出视图，和以 P 为输入执行真实搜索看到的视图不可区分，则称方案是 L 安全的。定义 $\mathrm{Real}_{\mathrm{A}}(s)$ 和 $\mathrm{Ideal}_{\mathrm{A,S}}(s)$ 如下。

$\mathrm{Real}_{\mathrm{A}}(s)$。挑战者输入安全参数生成密钥 k，利用密钥 k 和数据文件 D 生成密文索引 I 和密文数据 C，将 I 和 C 发送给攻击者 A。A 发起一定量查询 Q，其中每次查询关键字 w，A 会接收到 w 对应的令牌 TD，最后 A 返回比特 b 作为游戏输出。

$\mathrm{Ideal}_{\mathrm{A,S}}(s)$。给定 $L_1(D)$，模拟器 S 生成 (I^*,C^*) 并发送到 A。A 发起一定量查询 Q，其中每次查询关键字 w，模拟器 S 收到 $L_2(D,w)$，生成并返回对应的令牌 TD^*，最后 A 返回比特 b 作为游戏输出。

若对任意攻击者 A，足够大的 s 和多项式 p，存在模拟器 S，满足

$$\left|\Pr\left[\mathrm{Real}_{A}(s)=1\right]-\Pr\left[\mathrm{Ideal}_{A,S}(s)=1\right]\right|<\frac{1}{p(s)} \quad (9)$$

则可搜索加密方案对于 CKA2 具有 (L_1,L_2) 安全性。当 A 在游戏开始时就确定了查询 Q，即查询与索引以及之前的查询结果是独立的，则同样地可给出 CKA1 具有 (L_1,L_2) 安全性的定义。

针对密文搜索安全性定义，在本文设计的密文搜索过程中有以下定义。

1) L_1 安全性。密文搜索方案利用对称加密方式对数据进行加密，安全强度高，攻击者很难从密文中获取额外的信息。加密索引在边缘节点处生成，从而保证索引的安全性，使攻击者无法从密文索引中获得额外的信息。

2) L_2 安全性。在搜索过程中，查询关键字交给边缘节点，并在边缘节点处执行加密，加密后传送到云计算平台，从而向云端隐藏了关键字信息。在边缘节点构建密文索引时，针对每个关键字，利用填充节点确保不同关键字对应的搜索结果长度大致相同，从而即使攻击者获得了查询令牌和搜索结果的对应关系，也很难从返回结果获得有价值信息。当用户获得搜索结果后，一般情况下并不会向云服务器请求所有结果文档，而是检索其中部分特定文档，使攻击者不能得到一次查询对应于哪些文件，从而向攻击者隐藏了访问模式。

若攻击者预知部分加密文档内容，在泄露搜索模式或访问模式的情况下，攻击者利用先验知识会尝试获取到更多关于查询关键字或文档的信息[43-44]。通过将本文密文搜索方案构建模拟过程代入以上安全定义可看出，在文档加密和索引构建过程中，文档内容通过对称加密方式加密，密钥在边缘节点中存储，安全度较高，攻击者很难破解密文或获得密文对应的密钥。文档内容对应的搜索索引在边缘节点生成并加密，然后上传到云计算平台进行合并和搜索，攻击者无法解密密文索引，从而保护了索引数据的安全性。在搜索过程中，用户查询的关键字由边缘节点确定性加密，加密后上传到云计算平台执行查询操作，云计算平台返回搜索结果。在密文搜索方案中，文档标识符被随机性加密，利用填充节点使每个关键字的倒排列表含有的节点个数一致，保护搜索结果信息不被泄露，从而一定程度上向云计算平台隐藏了访问模式，即便攻击者拥有密文数据对应的明文数据信息，根据查询过程也无从得知其他的关键字或明文数据信息，满足 CKA2 安全性，具有 Le0 安全等级。

5　结束语

本文针对边缘计算数据安全问题，提出了一种密文搜索与共享方案，使在边缘节点处建立加密搜索索引，并同步到云计算平台，从而对索引作统一管理。同时本文设计密钥安全共享方案，以在不同边缘节点之间进行密文数据分享。

当然，本文设计的密文搜索与共享方案仍面临诸多问题，需进一步研究和改进。例如，本文假定用户侧的边缘节点是可信的，如果用户和边缘节点之间的可信度不高，则需要进一步利用脱密技术，如联邦学习、同态加密等处理之后再交给边缘节点执行。另外，由于加密索引在云计算平台进行管理，搜索过程中势必会泄露一定的数据信息，需要研究在搜索过程中增加一定的混淆措施，避免泄露关键字与搜索文档的对应关系。

参考文献：

[1] RGHIOUI A. Internet of things: visions, technologies, and areas of application[J]. Automation, Control and Intelligent Systems, 2017, 5(6): 83.

[2] 智研咨询. 2020 年全球及中国物联网产业发展现状及未来发展趋势分析[R]. 2021.
Zhiyan. 2020 global and Chinese Internet of things industry development status and future development trend analysis[R]. 2021.

[3] 西南证券. 2021 年物联网产业链全梳理[R]. 2021.
Southwest Securities. 2021 review on the IoT industry chain[R]. 2021.

[4] 头豹. 2021 年中国物联网指数系列报告一: 物联网概览-万物互联路在何方[R]. 2021.
Leadleo. 2021 China Internet of things index series report 1: overview of the Internet of things - where is the Internet of everything road[R]. 2021.

[5] GSMA 智库. 2021 中国移动经济发展报告[R]. 2021.
GSMA Intelligence. Report on 2021 China mobile economic development[R]. 2021.

[6] GRAY J. Distributed computing economics[J]. Queue, 2008, 6(3): 63-68.

[7] 赵梓铭, 刘芳, 蔡志平, 等. 边缘计算: 平台、应用与挑战[J]. 计算机研究与发展, 2018, 55(2): 327-337.
ZHAO Z M, LIU F, CAI Z P, et al. Edge computing: platforms, applications and challenges[J]. Journal of Computer Research and Development, 2018, 55(2): 327-337.

[8] 李林哲, 周佩雷, 程鹏, 等. 边缘计算的架构、挑战与应用[J]. 大数据, 2019, 5(2): 3-16.
LI L Z, ZHOU P L, CHENG P, et al. Architecture, challenges and applications of edge computing[J]. Big Data Research, 2019, 5(2): 3-16.

[9] 施巍松, 孙辉, 曹杰, 等. 边缘计算: 万物互联时代新型计算模型[J]. 计算机研究与发展, 2017, 54(5): 907-924.
SHI W S, SUN H, CAO J, et al. Edge computing: an emerging computing model for the Internet of everything era[J]. Journal of Computer Research and Development, 2017, 54(5): 907-924.

[10] HE W, AKHAWE D, JAIN S, et al. ShadowCrypt: encrypted web applications for everyone[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2014: 1028-1039.

[11] POPA R A, STARK E, HELFER J, et al. Building Web applications on top of encrypted data using Mylar[J]. IACR Cryptology EPrint Archive, 2016, 2016: 893.

[12] 方晨, 郭渊博, 王一丰, 等. 基于区块链和联邦学习的边缘计算隐私保护方法[J]. 通信学报, 2021, 42(11): 28-40.
FANG C, GUO Y B, WANG Y F, et al. Edge computing privacy protection method based on blockchain and federated learning[J]. Journal on Communications, 2021, 42(11): 28-40.

[13] 巫光福, 王影军. 基于区块链与云-边缘计算混合架构的车联网数据安全存储与共享方案[J]. 计算机应用, 2021, 41(10): 2885-2892.
WU G F, WANG Y J. Secure storage and sharing scheme of Internet of vehicles data based on hybrid architecture of blockchain and cloud-edge computing[J]. Journal of Computer Applications, 2021, 41(10): 2885-2892.

[14] KUMARI K A, SHARMA A, CHAKRABORTY C, et al. Preserving health care data security and privacy using Carmichael's theorem-based homomorphic encryption and modified enhanced homomorphic encryption schemes in edge computing systems[J]. Big Data, 2022, 10(1): 1-17.

[15] LU R X, HEUNG K, LASHKARI A H, et al. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT[J]. IEEE Access, 2017, 5: 3302-3312.

[16] WANG H Q, WANG Z W, DOMINGO-FERRER J. Anonymous and secure aggregation scheme in fog-based public cloud computing[J]. Future Generation Computer Systems, 2018, 78: 712-719.

[17] GUAN Z T, ZHANG Y, WU L F, et al. APPA: an anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT[J]. Journal of Network and Computer Applications, 2019, 125: 82-92.

[18] ZHANG R, ZHANG Y C, SUN J Y, et al. Fine-grained private matching for proximity-based mobile social networking[C]//2012 Proceedings IEEE INFOCOM. Piscataway: IEEE Press, 2012: 1969-1977.

[19] LIANG X H, LI X, ZHANG K, et al. Fully anonymous profile matching in mobile social networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 641-655.

[20] LYU L J, NANDAKUMAR K, RUBINSTEIN B, et al. PPFA: privacy preserving fog-enabled aggregation in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3733-3744.

[21] YAO A C. Protocols for secure computations[C]//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). Piscataway: IEEE Press, 1982: 160-164.

[22] 周俊, 沈华杰, 林中允, 等. 边缘计算隐私保护研究进展[J]. 计算机研究与发展, 2020, 57(10): 2027-2051.
ZHOU J, SHEN H J, LIN Z Y, et al. Research advances on privacy preserving in edge computing[J]. Journal of Computer Research and Development, 2020, 57(10): 2027-2051.

[23] SADEGHI A R, SCHNEIDER T, WEHRENBERG I. Efficient privacy-preserving face recognition[C]//International Conference on Information Security and Cryptology. Berlin: Springer, 2009: 229-244

[24] BRICKELL J, PORTER D E, SHMATIKOV V, et al. Privacy-preserving remote diagnostics[C]//Proceedings of the 14th ACM conference on Computer and communications security - CCS'07. New York: ACM Press, 2007: 498-507.

[25] DAMGÅRD I, FITZI M, KILTZ E, et al. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation[C]//Theory of Cryptography. Berlin: Springer, 2006: 285-304.

[26] NISHIDE T , OHTA K . Multiparty computation for interval, equality, and comparison without bit-decomposition protocol[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2007: 343-360.

[27] DINUR I, KELLER N, KLEIN O. An optimal distributed discrete log protocol with applications to homomorphic secret sharing[C]// Advances in Cryptology – CRYPTO 2018. Berlin: Springer, 2018: 824-873.

[28] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//Proceedings of 2000 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2000: 44-55.

[29] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[J]. Journal of Computer Security, 2011, 19(5): 895-934.

[30] 王娜, 郑坤, 付俊松, 等. 基于分块的移动边缘计算密文检索方法[J]. 通信学报, 2020, 41(7): 95-102.
WANG N, ZHENG K, FU J S, et al. Method of ciphertext retrieval in mobile edge computing based on block segmentation[J]. Journal on Communications, 2020, 41(7): 95-102.

[31] LI J Y, MA J F, MIAO Y B, et al. Verifiable semantic-aware ranked keyword search in cloud-assisted edge computing[J]. IEEE Transactions on Services Computing, 2021: doi.org/10.1109/TCS.2021.3098864.

[32] LIU Q. Fog/edge computing for security, privacy, and applications[M]. Berlin: Springer, 2021.

[33] KAMARA S, PAPAMANTHOU C, ROEDER T. Dynamic searchable symmetric encryption[C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security. New York: ACM Press, 2012: 965-976.

[34] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522.

[35] LIU Q, WANG G J, WU J. Secure and privacy preserving keyword searching for cloud storage services[J]. Journal of Network and Computer Applications, 2012, 35(3): 927-933.

[36] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology. Berlin: Springer, 1984: 47-53.

[37] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology - CRYPTO 2001. Berlin: Springer, 2001: 213-229.

[38] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]//Proceedings of the 22nd International Conference on Theory and applications of Cryptographic Techniques. Berlin: Springer, 2003: 272-293.

[39] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology - ASIACRYPT 2003. Berlin: Springer, 2003: 452-473.

[40] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568-588.

[41] SAIDI A, NOUALI O, AMIRA A. SHARE-ABE: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and fog computing[J]. Cluster Computing, 2022, 25(1): 167-185.

[42] ZHANG J H, WU M L, ZHANG Q J, et al. A lightweight data sharing scheme with resisting key abuse in mobile edge computing[C]//Proceedings of IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops. Piscataway: IEEE Press, 2021: 1-6.

[43] ISLAM M S, KUZU M, KANTARCIOGLU M. Access pattern disclosure on searchable encryption: ramification, attack and mitigation[J]. Ndss, 2012, 20: 1-15.

[44] CASH D, GRUBBS P, PERRY J, et al. Leakage-abuse attacks against searchable encryption[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 668-679.

[45] MICALI S. Scalable certificate validation and simplified PKI management[C]//Proceedings of the 1st Annual PKI Research Workshop. Dartmouth: [s.n.], 2002: 15-25.

[46] TRIDGELL A, MACKERRAS P. The RSYNC algorithm[R]. 1996.

[47] 刘子杰, 王凯, 王亚刚, 等. 工业互联网端边云协同数据同步方案设计与实现[J]. 计算机应用研究, 2022, 39(3): 821-825.
LIU Z J, WANG K, WANG Y G, et al. Design and implementation of end-to-end cloud collaborative data synchronization scheme for industrial Internet[J]. Application Research of Computers, 2022, 39(3): 821-825.

[作者简介]

王继锋（1969− ），男，陕西咸阳人，国网汇通金财（北京）信息科技有限公司高级工程师，主要研究方向为电子商务、信息安全。

王国峰（1988− ），男，山东济宁人，博士，朗新科技集团股份有限公司高级工程师，主要研究方向为网络安全。

收录声明

本刊对发表的文章，拥有出版电子版、网络版版权，并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Journal on Communications has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果，无一稿多投；论文内容不涉及国家机密；未曾以任何形式用任何文种在国内外公开发表过；论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题，论文作者将承担全部责任。

The authors of *Journal on Communications* guarantee that their submitted articles are original and contain nothing confidential. The said article is only submitted to *Journal on Communications*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

通信学报

Journal on Communications

发行代号：国内2-676 / 国外M395

2022年4月25日出版　定价：98.00元

ISSN 1000-436X

CN 11-2102/TN