·网络空间安全·　　文章编号：1000-3428(2023)12-0121-08　　文献标志码：A　　中图分类号：TP309

云边协同下可排序的属性基可搜索加密方案

王　正，曹素珍，赵　晓，周大伟，邢丹丹

（西北师范大学 计算机科学与工程学院，兰州 730070）

摘　要：云计算和边缘计算技术可以有效解决网络边缘流量爆炸式增长带来的巨大存储和计算需求，但数据外包后用户的敏感信息可能会因云端和边缘设备的不完全可信出现泄露问题。为了解决该问题，提出云边协同下可排序的属性基可搜索加密方案。采用云边协同技术，将大量的密文存储到云服务器，使与其对应的加密索引上传到距离最近的边缘节点进行多关键字搜索和辅助解密，提高通信效率。采用TF-IDF规则使搜索结果中仅返回最符合用户需求的Top-k文件，从而实现多关键字排序。将用户的属性分为属性值和属性名，仅公开属性名，从而通过隐藏属性值的方式达到保护用户敏感信息的目的，同时采用在线/离线混合加密技术降低用户计算开销。基于DBDH和q-parallel DBDH假设证明了该方案在随机预言模型中的选择关键字攻击下满足不可区分性。分析结果表明，该方案在加密和陷门生成阶段的计算开销相比于次优方案降低了10%和25%，同时在解密阶段保持恒定，具有更高的密文检索效率。

关键词：边缘计算；TF-IDF规则；可搜索加密；属性加密；策略隐藏

开放科学（资源服务）标志码（OSID）：

中文引用格式：王正，曹素珍，赵晓，等. 云边协同下可排序的属性基可搜索加密方案[J]. 计算机工程，2023，49(12)：121-128.

英文引用格式：WANG Z，CAO S Z，ZHAO X，et al. Sortable attribute-based searchable encryption scheme under cloud-edge collaboration[J].Computer Engineering，2023，49(12)：121-128.

Sortable Attribute-Based Searchable Encryption Scheme Under Cloud-Edge Collaboration

WANG Zheng，CAO Suzhen，ZHAO Xiao，ZHOU Dawei，XING Dandan

（College of Computer Science and Engineering，Northwest Normal University，Lanzhou 730070，China）

【Abstract】Cloud and edge computing technologies can effectively solve the complex storage and computing needs of the explosive growth of network edge traffic. However，after data outsourcing，users' sensitive information may be leaked due to incomplete trust in cloud and edge devices. An Attribute-Based Searchable Encryption（ABSE）scheme with cloud-edge collaboration is proposed to solve this problem. Cloud-edge collaboration technology is adopted to store many ciphertexts on the cloud server，and the corresponding encryption index is uploaded to the nearest edge node for multi-keyword search and auxiliary decryption to improve communication efficiency. The TF-IDF rule is used to return only the Top-k files that meet the users' needs in the search results，hence the multi-keyword sorting. The user attribute is divided into value and name，and only the attribute name is disclosed to protect the users' sensitive information by hiding the attribute value. At the same time，online/offline hybrid encryption technology is used to reduce the users' computing overhead. Based on DBDH and q-parallel DBDH hypothesis，the proposed scheme is proved to be INDistinguishable against Chosen Keyword Attack（IND-CKA）in the random prediction model. According to the analysis of experimental results，compared with a suboptimal scheme，the computational overhead of this scheme is reduced by 10% and 25%. Simultaneously，the scheme remains constant in the decryption stage and has higher efficiency and practicability of ciphertext retrieval.

【Key words】edge computing；TF-IDF rule；Searchable Encryption（SE）；attribute encryption；policy hiding

DOI：10. 19678/j. issn. 1000-3428. 0067398

基金项目：国家自然科学基金（62262060）；甘肃省教育厅产业支撑计划项目（2022CYZC-17）。

作者简介：王　正（1998—），女，硕士研究生，CCF学生会员，主研方向为网络与信息安全；曹素珍，副教授；赵　晓、周大伟、邢丹丹，硕士研究生。

收稿日期：2023-04-13　　**修回日期：**2023-06-27　　**E-mail：**835419380@qq.com

0 概述

随着物联网和5G技术的广泛应用[1-2]，现有云服务器的性能已不能满足互联网时代对海量数据的实时处理需求。边缘设备[3-4]以低时延、移动性支持等优势逐步成为解决上述问题的一种新途径。云服务器和边缘设备是半诚实的[5-7]，因此为保证用户数据的机密性，数据所有者（Data Owner，DO）通常将数据加密后再存储于云端或边缘设备，然而如何检索密文成为数据用户面临的一大难题。文献[8]提出可搜索加密（Searchable Encryption，SE）概念，有效解决了密文检索的难题。

在早期的SE方案中常采用单关键字SE方案[9]，但因存在大量的关键字索引重复问题，从而导致搜索效率不高。为了提高搜索的准确性，在后续的研究中用户搜索的关键字通常采取多关键字方案[10-12]。文献[13]提出一种多关键字SE方案，通过匹配多关键字的索引和搜索陷门来提高搜索效率，但仍存在关键字与主题相关性不大的问题。文献[14]提出一种多关键字排序SE算法，利用TF-IDF规则根据关键字相关的程度排序搜索结果，仅返回最满足用户需求的Top-k文件。上述文献无论是采用对称或非对称加密算法均无法满足数据共享时的细粒度访问控制需求。

文献[15]提出属性基可搜索加密（Attribute-Based Searchable Encryption，ABSE）概念，实现了外包加密数据上的安全搜索和细粒度访问控制。文献[16-17]提出一种基于密文策略的ABSE方案（CP-ABSE），在CP-ABSE方案中私钥与属性相关联，密文与访问结构相关联，使得访问密文的用户由数据所有者设定的访问策略决定，达到细粒度访问控制的效果。KP-ABSE[18]方案是将策略嵌入用户密钥，属性嵌入密文，但这两种ABSE方案都可能存在访问策略泄露问题。文献[19]提出一种基于隐藏策略和外包解密的白盒可跟踪属性加密方案，基于LSSS访问结构，该方案采用策略隐藏的方式只对属性名进行公开，缺陷在于不支持对多关键字的搜索排序，搜索结果不精准。文献[20-21]提出一种基于边缘计算框架的高效密文索引检索方案，结合可搜索加密技术与边缘计算技术所定义的边缘缓存网络模型使密文检索更加安全高效。文献[22]提出IIoT时代可持续边缘云网络的多关键词排序搜索隐私保护方案，但该方案无法满足大规模计算需求。

针对上述问题，本文提出云边协同下可排序的属性基可搜索加密方案，主要工作如下：

1）利用云边协同技术，将加密后的数据上传到云端，与其对应的加密索引上传到最近的边缘节点，提高了搜索效率，降低了用户的计算负担。

2）用户的属性由属性名和属性值组成，在构造访问结构时，用户仅通过公开的属性名进行陷门搜索匹配，从而使得未经授权的用户无法获取访问策略中的任何有效信息。

3）在密文检索阶段，可在排除无关关键字的情况下根据检索关键字的重要程度进行排序，最终返回与用户需求最相关的Top-k密文，实现了多关键字排序搜索。

4）利用在线/离线加密技术，数据所有者在上传密文之前先进行离线加密，降低客户端的计算成本。

1 预备知识

1.1 双线性映射

选择两个循环群G_1、G_2，p是它们的素数阶，定义一个双线性映射$e: G_1 \times G_1 \to G_2$满足以下性质[23]：

1）双线性。对$\forall x,y \in G_1, \forall a,b \in Z_p^*$，有$e\left(x^a,y^b\right)=e\left(x^b,y^a\right)=e\left(x,y\right)^{ab}$成立。

2）非退化性。$\exists x,y \in G_1$满足$e\left(x,y\right) \neq 1$。

3）可计算性。对$\forall x,y \in G_1$，存在一个多项式时间算法有效计算$e\left(x,y\right)$。

1.2 访问结构

设$P=\left\{P_1,P_2,\cdots,P_n\right\}$表示参与者的集合，令$2^P=\left\{A|A\subseteq\left\{P_1,P_2,\cdots,P_n\right\}\right\}$，集合$A\subseteq 2^P$是单调的，当且仅当对于任意子集$B,C\subseteq P$，如果$B\in A$且$B\subseteq C$，则$C\in A$。若$A$是$P=\left\{P_1,P_2,\cdots,P_n\right\}$中的非空子集（单调的），即$A\subseteq 2^{\left\{P_1,P_2,\cdots,P_n\right\}}\backslash\varnothing$，则称$A$是一个访问结构（单调的）。对于任意集合$D$，若$D\in A$，则$D$为授权集，否则为非授权集[24]。

1.3 线性秘密共享方案

定义P上的一个线性秘密共享方案π，满足如下条件[25]：

1）Z_P^*上的向量可以由参与实体所拥有的秘密份额组成。

2）每个线性秘密共享方案都有一个$l\times n$的生成矩阵$\boldsymbol{M}$，且存在单射函数$\rho:\{1,2,\cdots,l\}\to P$把$\boldsymbol{M}$的每一行$\left(i=1,2,\cdots,l\right)$映射到参与者$\rho(i)$。考虑向量$\boldsymbol{v}=\left(s,v_2,v_3,\cdots,v_n\right)$，$s\in Z_P^*$是共享秘密值，选择随机数$v_2,v_3,\cdots,v_n\in Z_P^*$隐藏共享秘密值$s$，则$\boldsymbol{Mv}$是共享秘密份额，其中$\lambda_i=\left(\boldsymbol{Mv}\right)_i$是共享秘密值$s$的第$i$个秘密份额。

1.4 TF-IDF规则

TF-IDF用来评估指定关键字对于文档集合中某一篇文档的重要程度[26]，值越大，说明该关键字w在文档f中的重要程度越靠前。TF是计算指定关键字w在查询文档f中出现的次数，IDF是该关键词出现在所有文档中的数据集合。根据下述拆分规则计算Top-k文件。

拆分规则：基于随机的n维二进制向量$\boldsymbol{P}$计算n维向量$\boldsymbol{Q}$，利用$\boldsymbol{P}$将$\boldsymbol{Q}$拆分为两个随机向量$\left(\boldsymbol{Q}',\boldsymbol{Q}''\right)$，如式（1）所示：

$$\begin{cases}\boldsymbol{Q}',\boldsymbol{Q}''\text{是2个满足}\boldsymbol{Q}'+\boldsymbol{Q}''=\boldsymbol{Q}_j\text{的随机值},\boldsymbol{P}_j=0\\ \boldsymbol{Q}'=\boldsymbol{Q}''=\boldsymbol{Q}_j,\boldsymbol{P}_j=1\end{cases} \tag{1}$$

1.5　困难问题假设

困难问题假设具体如下：

1）DBDH假设。设一个循环群G，p是它的素数阶，g是G的一个生成元。随机选择$a,b,c,z\in Z_p$，给定多元组$\left(g,g^a,g^b,g^c,e\left(g,g\right)^{abc}\right)$，如果不存在一种算法能够在多项式时间内以不可忽略的概率区分$\left(g,g^a,g^b,g^c,z\right)$，则DBDH假设成立。

2）q-parallel DBDH假设。选择两个乘法循环群G_1、G_2，p是它们的素数阶，g是G_1的一个生成元。随机选择$q+2$个元素$x,a,b_1,b_2,\cdots,b_q\in Z_p$，计算：

$$A=\left\{g,g^a,g^x,\cdots,g^{x^q},g^{x^{q+2}},\cdots,g^{x^{2q}}\left\{g^{ab_j},g^{x/b_j},\cdots,g^{x^q/b_j},g^{x^{q+2}/b_j},\cdots,g^{x^{2q}/b_j}\right\}_{\forall j\in[q]}\left\{g^{xab_i/b_j},\cdots,g^{x^q ab_i/b_j}\right\}_{\forall i,j\in[q],i\neq j}\right\}$$

给定$\left(A,e\left(g,g\right)^{x^{q+1}a}\right)$，如果不存在一种概率多项式算法能够在多项式时间内以不可忽略的优势区分$\left(A,Z\right)$，其中$Z\in G_2$，则假设成立。

1.6　符号描述

文中使用的一些符号和变量如表1所示。

表1　符号和变量描述

Table 1　Description of symbols and variables

符号	说明
G_1、G_2	p阶循环群
Z_p^*	去除0的模p整数群
e	双线性映射
H	哈希函数
G_{P}	全局参数
K_{M}	系统主密钥
$\mathcal{A}$	攻击者
$\mathcal{C}$	挑战者
U	全局属性集合
$(\boldsymbol{M},\rho)$	访问策略（$\boldsymbol{M}$是一个矩阵，ρ是一个映射函数）

2　属性基可搜索加密方案

2.1　系统模型

所提方案的系统主要包括5类实体，分别是授权机构（Authorization Attribute，AA）、云服务提供商（Cloud Service Provider，CSP）、边缘节点（Edge Node，EN）、数据所有者和数据用户（Data User，DU）。

该方案由一个受信任的AA公开发布全局参数并对主密钥保密，DO将加密文件上传到CSP存储，将相应的关键字索引上传到最近的EN。DU根据访问策略生成搜索陷门发送给最近的EN，EN接收到搜索陷门后先对CSP中存储的数据进行搜索，CSP搜索出符合的文件返回给EN，EN利用用户生成的部分解密密钥对其进行部分解密，将Top-k文件返回给用户解密，最后得到共享的数据文件。系统模型及流程如图1所示。

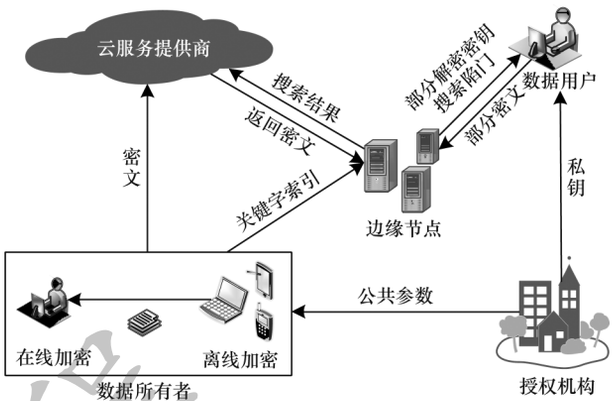

图1　系统模型及流程

Fig.1　System model and procedure

该模型在现实应用中可适应于大部分实际场景，如智能电网。假设电力运营公司使用该模型使某市的各小区之间可相互共享一些电网用户数据。电网用户查看自己相关的数据时只需要简单的身份注册，受信任的授权机构根据其基本信息分发可解密本人数据的属性密钥。电网用户根据属性设置访问策略，系统将其转换为一个矩阵并将其嵌入密文后上传云服务器，相应的关键字索引上传到最近的边缘节点。管理人员等其他想要访问数据的电网查询者需要受信任的授权机构审核其身份信息并为其分发属性密钥，在系统中输入相关关键字，当属性满足电网用户设置的访问策略时，则可解密搜索结果，否则无权查看，这在一定程度上保护了数据隐私。

1）AA。AA是一个完全受信任的实体，由它生成全局参数和系统主密钥，当用户想要查询时，可以根据其属性集生成对应的用户私钥。

2）CSP。CSP是一个诚实但好奇的半可信实体，会好奇云上存储的数据但会诚实地执行任务。在该系统中，允许系统中的合法用户上传或访问存储其上的密文数据。

3）EN。EN用于存储密文索引，当从DU接收搜索陷门时，诚实地执行搜索算法，并将搜索结果发送到CSP。在获得从CSP返回的加密文件后，协助DU进行部分密文解密操作，并根据TF-IDF规则计算并返回给用户最符合要求的Top-k文件。

4）DO。根据DO设定的访问策略对数据和关键字进行加密后上传到EN。

5）DU。每个DU计算搜索陷门并发送到边缘节点进行匹配查询，生成部分解密密钥发送到边缘节点以供对返回的搜索结果进行部分解密操作。

2.2　安全模型

所提方案的安全模型通过攻击者$\mathcal{A}$和挑战者$\mathcal{C}$之间的模拟游戏定义。若攻击者$\mathcal{A}$在多项式时间算法内不能以不可忽略的优势在游戏中获胜，则该方案具有选择关键字攻击（IND-CKA）安全性。

1)初始化。挑战者$\mathcal{C}$调用SetUp算法,通过安全参数λ计算得全局参数G_{P}和系统主密钥K_{M}。

2)查询阶段1。攻击者$\mathcal{A}$向挑战者$\mathcal{C}$请求对应属性集$S_{\mathcal{A}}$的私钥和待查询关键字的集合W'的搜索陷门。

3)挑战。攻击者$\mathcal{A}$向挑战者$\mathcal{C}$发送两个大小相同的关键字w_1、w_2,攻击者$\mathcal{A}$提供访问策略$(\boldsymbol{M},\rho)$,挑战者$\mathcal{C}$随机选择$b\in\{0,1\}$,利用w_b生成加密关键字索引I_{w_b}返回给攻击者$\mathcal{A}$。

4)查询阶段2。攻击者$\mathcal{A}$重复进行查询阶段1,查询更多与w_1、w_2不同的关键字集合的搜索陷门。

5)猜测阶段。攻击者$\mathcal{A}$输出b的一个猜想$b'\in\{0,1\}$,若$b=b'$,则攻击者$\mathcal{A}$获胜,攻击者$\mathcal{A}$成功的优势为$A_{\mathrm{dv}}=\left|\Pr[b=b']-\frac{1}{2}\right|$。

2.3 算法描述

算法描述具体如下:

1)设置$\mathrm{SetUp}(1^{\lambda})\rightarrow(G_{\mathrm{P}},K_{\mathrm{M}})$。AA执行该算法,输入安全参数$\lambda$,输出全局参数$G_{\mathrm{P}}$,主密钥$K_{\mathrm{M}}$。

2)密钥生成$\mathrm{KeyGen}(G_{\mathrm{P}},K_{\mathrm{M}},S)\rightarrow(K_S)$。AA执行该算法,输入全局参数$G_{\mathrm{P}}$,根据主密钥$K_{\mathrm{M}}$和用户的属性集$S$生成用户的属性密钥$K_S$。

3)加密。加密包括离线加密和在线加密。

(1)离线加密$\mathrm{Offline.Enc}(G_{\mathrm{P}})\rightarrow(C_{\mathrm{P}})$。在没有确定关键字集合以及访问策略之前,DO空闲时执行该算法,输入全局参数G_{P},根据用户属性S及选择的秘密值s输出中间密文C_{P},用于在线加密。

(2)在线加密$\mathrm{Online.Enc}(G_{\mathrm{P}},C_{\mathrm{P}},F,W,A(\boldsymbol{M},\rho))\rightarrow(C_{\mathrm{T}},I_w)$。DO执行该算法,输入全局参数$G_{\mathrm{P}}$,离线加密时生成的中间密文$C_{\mathrm{P}}$,明文文件集$F$,关键字集合$W$,访问策略$A(m,\rho)$,输出对数据加密生成的加密密文$C_{\mathrm{T}}$和对关键字加密生成的加密索引$I_w$,并根据TF-IDF规则计算索引向量$\boldsymbol{I}_w$。

4)陷门生成$\mathrm{Trapdoor}(G_{\mathrm{P}},K_S,q)\rightarrow(T_q)$。DU执行该算法,输入用户私钥$K_S$和在关键字集合中随机选择的待搜索关键字$q$,生成查询陷门用于密文搜索。同时,根据TF-IDF规则计算查询向量与在线加密时生成的索引向量一同用于Top-k文件的分数排序计算。

5)密文搜索$\mathrm{Search}(G_{\mathrm{P}},C_{\mathrm{T}},I_w,T_q)\rightarrow(C_{\mathrm{T}}/\perp)$。CSP执行该算法,输入查询陷门$T_q$和关键字索引$I_w$,检测其能否成功匹配,若能则继续验证,否则终止。

6)验证Verify。验证返回结果的正确性,并根据TF-IDF规则计算并返回给用户需要的Top-k文件。

7)转换$\mathrm{Transform}(G_{\mathrm{P}},K_S)\rightarrow(K_{\mathrm{P}})$。由DU执行该算法,输入DU的私钥$K_S$,输出边缘节点的部分解密密钥$K_{\mathrm{P}}$,用于协助密文的部分解密。

8)部分解密密文$\mathrm{E.Dec}(G_{\mathrm{P}},K_{\mathrm{P}},C_{\mathrm{T}})\rightarrow(C_{\mathrm{PT}})$。EN执行该算法,输入全局参数$G_{\mathrm{P}}$和边缘节点的部分解密密钥$K_{\mathrm{P}}$,对所得的Top-$k$文件密文进行部分解密,输出部分解密密文$C_{\mathrm{PT}}$。

9)解密$\mathrm{Dec}(K_S,C_{\mathrm{PT}},K_\tau)\rightarrow(m)$。DU执行该算法,输入DU的私钥$K_S$,并利用中间解密密钥中包含的转换因子$K_\tau$,对步骤8)得到的部分解密密文$C_{\mathrm{PT}}$解密后,获得所需明文$m$。

2.4 方案构造

方案构造具体如下:

1)系统建立。先初始化系统,输入安全参数λ,设置全局参数$U=\{1,2,\cdots,N\}$,设两个乘法循环群G_1、G_2,p是它们的素数阶,设定双线性对$e:G_1\times G_1\rightarrow G_2$,其中,$g$是$G_1$的生成元,并选择哈希函数$H:\{0,1\}^*\rightarrow Z_p^*$。AA随机选择$\alpha,\beta,\mu\in Z_p^*$,计算$e(g,g)^{\alpha}$、$g^{\beta}$、$g^{\mu}$。对于每个属性$i\in U$,AA随机选择$a_i\in Z_p^*$,计算$T_i=g^{a_i}$。最后生成系统的全局参数$G_{\mathrm{P}}$和主密钥$K_{\mathrm{M}}$,如式(2)所示:

$$\begin{cases}G_{\mathrm{P}}=\left\{G_1,G_2,g,p,e(g,g)^{\alpha},g^{\beta},g^{\mu},H,T_i\right\}_{i\in U}\\K_{\mathrm{M}}=\{\alpha,\beta,\mu\}\end{cases}\tag{2}$$

其中:G_{P}由AA公开;K_{M}由AA秘密保存。

2)密钥生成。AA输入全局参数G_{P}和属性集合S,包含j个属性,AA随机选择$x\in Z_p^*$,计算用户密钥$K_1=g^x$,对每个属性$j\in S$选择随机数$x_j\in Z_p^*$,计算属性密钥,如式(3)所示。最后生成私钥$K_S=\left\{K_1,K_2,K_3,K_i\right\}_{i\in S}$发送给DU。

$$\begin{cases}K_2=g^{\frac{\alpha}{\beta}}g^{\frac{\mu x_j}{\beta}}\\K_3=g^{x_j}\\K_i=(T_i)^{x_j}\end{cases}\tag{3}$$

3)离线加密。在没有确定关键字集合以及访问策略之前先进行离线计算。DO选择秘密值$s\in Z_p^*$,计算密文,如式(4)所示:

$$\begin{cases}C_1=e(g,g)^{\alpha s}\\C_2=g^{\beta s}\\C=m\times C_1=m\times e(g,g)^{\alpha s}\end{cases}\tag{4}$$

对于每个属性$i\in U$,随机选择$y_i\in Z_p^*$,计算$C_i=T_i^{y_i}$、$D_i=g^{-y_i}$,最后输出中间密文$C_{\mathrm{P}}=\left\{s,C_1,C_2,C,C_i,D_i\right\}_{i\in U}$。

4)在线加密。设$l\times n$的访问矩阵$\boldsymbol{M}_{l\times n}$,其中对$\forall i\in[1,l]$,$\boldsymbol{M}_i$是矩阵$\boldsymbol{M}$的第$i$行,定义函数$\rho$将第$i$行映射到相应的属性名$a_i$,$\rho:\rho(i)\rightarrow a_i$。最后将$\left\{\boldsymbol{M}_{l\times n},\rho\right\}$以明文的形式作为访问结构。

(1)数据加密

①DO随机选择一个秘密值$s\in Z_p^*$和一个向量$\boldsymbol{v}=(s,v_2,v_3,\cdots,v_n)^{\mathrm{T}}\in Z_p^*$。

②计算$\lambda_i=\boldsymbol{M}_{l\times n}\times\boldsymbol{v}$。

③对每个属性进行加密，计算 $C_i'=g^{\mu\lambda_i}$，$C_i''=H\left(\{\rho(i):b_i\}\right)^{\lambda_i}$。

(2)关键字加密。$\forall w_j\in W\left(j\in 1,2,\cdots,d\right)$，其中 j 是 W 中的关键字。DU随机选择 $r\in Z_p^*$，计算 $I_1=g^r$、$I_2=g^{\beta r}$、$I_3=g^{\mu r}$，如果关键字包含在文件中，则计算 $I_{w_j}=\sum_{j=1}^{d}g^{H(w_j)\mu r}$，否则计算 $I_{w_j}=1$。

(3)生成索引向量。DO根据拆分规则式(1)设置索引向量 $\boldsymbol{Q}=\left\{\boldsymbol{M}_1^{\mathrm{T}}\boldsymbol{Q}',\boldsymbol{M}_2^{\mathrm{T}}\boldsymbol{Q}''\right\}$，与关键字索引一同作为密文索引发送到EN。

5)查询

(1)生成查询陷门。DU选择关键字集合 W，随机选择 q，计算查询陷门如式(5)所示：

$$\begin{cases}T_1=g^q\\ T_2=\prod_{j=1}^{d}g^{H(w_j)q}\\ T_3=\prod_{j=1}^{d}g^{H(w_j)\beta q}\end{cases}\tag{5}$$

(2)生成查询向量。DU根据拆分规则式(1)设置查询向量 $\boldsymbol{O}=\left\{\boldsymbol{M}_1^{-1}\boldsymbol{O}'\boldsymbol{M}_2^{-1}\boldsymbol{O}''\right\}$，将其与查询陷门一起发送到EN。

6)密文搜索。EN检测查询陷门与关键字索引能否成功匹配，验证等式 $e\left(I_{w_j},T_1\right)e\left(I_1,T_3\right)=e\left(I_2\times I_3,T_2\right)$ 是否成立，若成立则使用式(6)计算索引向量和查询向量的相关分数：

$$S_{\mathrm{Score}}=\boldsymbol{Q}\times\boldsymbol{O}=\left\{\boldsymbol{M}_1^{\mathrm{T}}\boldsymbol{Q}',\boldsymbol{M}_2^{\mathrm{T}}\boldsymbol{Q}''\right\}\times\boldsymbol{O}=\left\{\boldsymbol{M}_1^{-1}\boldsymbol{O}',\boldsymbol{M}_2^{-1}\boldsymbol{O}''\right\}\tag{6}$$

将计算得到的相关分数结果排序，仅返回Top-k文件密文CT，否则输出⊥。

7)中间解密密钥。在搜索成功后，DU随机选择 $\tau\in Z_p^*$，计算 $K_\tau=g^\tau$，$K_4=K_2\times K_\tau=\left(g^{\frac{\alpha}{\beta}}g^{\frac{\mu x_j}{\beta}}\right)\times g^\tau$。最后得到中间解密密钥 $K_{\mathrm{P}}=\left\{K_\tau=g^\tau,K_3=g^{x_j},K_4=K_2\times K_\tau=\left(g^{\frac{\alpha}{\beta}}g^{\frac{\mu x_j}{\beta}}\right)\times g^\tau\right\}_{\forall i\in S}$ 并将其发送给边缘节点。

8)部分解密。边缘节点接收中间解密密钥 K_{P} 和搜索成功的密文 C_{T} 并对 C_{T} 进行部分解密。DU上传属性名 a_i，DO上传映射函数 $\rho:\rho(i)\to a_i$，当用户的属性名满足访问策略时，存在一组常数 $\left\{\omega_i\in Z_p^*\right\}_{i\in d'}$ 使 $\sum_{i=1}^{d'}\lambda_i\omega_i=s$。计算部分解密密文 $C_{\mathrm{PT}}=\dfrac{e\left(C_2,K_4\right)}{\left(\prod_{i\in a_{\mathrm{att}}}e\left(C_i\times C_i',K_3\right)e\left(K_i,D_i\right)^{\omega_i}\right)}=e\left(g,g\right)^{\alpha s}e\left(g,g\right)^{\beta s\tau}$。

9)明文。DU收到EN返回的部分解密密文 C_{PT} 后，计算明文 $m=\dfrac{C\times e\left(C_2,K_\tau\right)}{C_{\mathrm{PT}}}$ 并输出。

3　正确性与安全性证明

3.1　正确性证明

1)关键字匹配正确性

检查式(7)是否成立来判断用户生成的陷门和密文对应的关键字是否匹配：

$$e\left(I_{w_j},T_1\right)e\left(I_1,T_3\right)=e\left(I_2\times I_3,T_2\right)\tag{7}$$

等式左边推导如下：

$$e\left(I_{w_j},T_1\right)e\left(I_1,T_3\right)=e\left(\sum_{j=1}^{d}g^{H(w_j)\mu r},g^q\right)e\left(g^r,\prod_{j=1}^{d}g^{H(w_j)\beta q}\right)=e\left(g,g\right)^{\mu rq\prod_{j=1}^{d}H(w_j)}e\left(g,g\right)^{\beta rq\prod_{j=1}^{d}H(w_j)}$$

等式右边推导如下：

$$e\left(I_2\times I_3,T_2\right)=e\left(g^{\beta r}\times g^{\mu r},\prod_{j=1}^{d}g^{H(w_j)q}\right)=e\left(g^{\beta r},\prod_{j=1}^{d}g^{H(w_j)q}\right)e\left(g^{\mu r},\prod_{j=1}^{d}g^{H(w_j)q}\right)=e\left(g,g\right)^{\mu rq\prod_{j=1}^{d}H(w_j)}e\left(g,g\right)^{\beta rq\prod_{j=1}^{d}H(w_j)}$$

综上，关键字匹配的正确性得证。

2)解密密文正确性

边缘节点接收到DU的部分解密密钥后计算部分解密密文。边缘节点辅助解密的正确性证明如下：

$$C_{\mathrm{PT}}=\frac{e\left(C_2,K_4\right)}{\prod_{i\in a_{\mathrm{att}}}e\left(C_i\times C_i',K_3\right)e\left(K_i,D_i\right)^{\omega_i}}=\frac{e\left(g^{\beta s},\left(g^{\frac{\alpha}{\beta}}g^{\frac{\mu x_j}{\beta}}\right)\times g^\tau\right)}{\prod_{i\in a_{\mathrm{att}}}e\left(T_i^{y_i}\times g^{\mu\lambda_i},g^{x_j}\right)e\left(T_i^{x_j},g^{-y_i}\right)^{\omega_i}}=\frac{e\left(g^{\beta s},\left(g^{\frac{\alpha}{\beta}}g^{\frac{\mu x_j}{\beta}}\right)\right)e\left(g^{\beta s},g^\tau\right)}{\prod_{i\in a_{\mathrm{att}}}e\left(T_i^{y_i},g^{x_j}\right)e\left(g^{\mu\lambda_i},g^{x_j}\right)e\left(T_i^{x_j},g^{-y_i}\right)^{\omega_i}}=\frac{e\left(g^{\beta s},g^{\frac{\alpha}{\beta}}\right)e\left(g^{\beta s},g^{\frac{\mu x_j}{\beta}}\right)e\left(g^{\beta s},g^\tau\right)}{\prod_{i\in a_{\mathrm{att}}}e\left(g^{\mu\lambda_i},g^{x_j}\right)^{\omega_i}}=\frac{e\left(g,g\right)^{s\alpha}e\left(g,g\right)^{s\mu x_j}e\left(g,g\right)^{\beta s\tau}}{\prod_{i\in a_{\mathrm{att}}}e\left(g,g\right)^{\omega_i\mu\lambda_i x_j}}=\frac{e\left(g,g\right)^{s\alpha}e\left(g,g\right)^{s\mu x_j}e\left(g,g\right)^{\beta s\tau}}{e\left(g,g\right)^{s\mu x_j}}=e\left(g,g\right)^{\alpha s}e\left(g,g\right)^{\beta s\tau}$$

根据上述可得解密密文的正确性证明如下：

$$m=\frac{C\times e\left(C_2,K_\tau\right)}{P_{\mathrm{PCT}}}=\frac{m\times e\left(g,g\right)^{\alpha s}e\left(g^{\beta s},g\tau\right)}{e\left(g,g\right)^{\alpha s}e\left(g,g\right)^{\beta s\tau}}=\frac{m\times e\left(g,g\right)^{\alpha s}e\left(g,g\right)^{\beta s\tau}}{e\left(g,g\right)^{\alpha s}e\left(g,g\right)^{\beta s\tau}}=m$$

综上，解密密文的正确性得证。

3.2 安全性证明

定理1 若多项式时间内的算法允许攻击者$\mathcal{A}$以可忽略的优势获胜，则该方案具有IND-CKA安全性。

1）初始化。输入安全参数λ，选择一个循环群G_1，p是它的素数阶，g是G_1的生成元，随机选择$\alpha,\beta,\mu\in Z_p^*$和哈希函数$H:\{0,1\}^*\to Z_p^*$，挑战者$\mathcal{C}$调用$\mathrm{SetUp}\left(1^\lambda\right)\to\left(G_{\mathrm{P}},K_{\mathrm{M}}\right)$算法。最后生成系统的全局参数$G_{\mathrm{P}}$和主密钥$K_{\mathrm{M}}$，$G_{\mathrm{P}}$由AA公开，$K_{\mathrm{M}}$由AA秘密保存。

$$\begin{cases}G_{\mathrm{P}}=\left\{G_1,G_2,g,p,e\left(g,g\right)^{\alpha},g^{\beta},g^{\mu},H,T_i\right\}_{i\in U}\\K_{\mathrm{M}}=\left\{\alpha,\beta,\mu\right\}\end{cases}$$

2）查询阶段1。查询阶段1包括私钥查询和陷门查询。

（1）私钥查询。攻击者$\mathcal{A}$向挑战者$\mathcal{C}$请求对应属性集$S_{\mathcal{A}}$的私钥且S不满足访问策略$\left(\boldsymbol{M},\rho\right)$，挑战者$\mathcal{C}$随机选择$x\in Z_p^*$，计算用户密钥$K_1=g^x$，对每个属性$j\in S$选择随机数$x_j\in Z_p^*$，计算属性密钥$K_2=g^{\frac{\alpha}{\beta}}g^{\frac{\mu x_j}{\beta}}$、$K_3=g^{x_j}$、$K_i=\left(T_i\right)^{x_j}$，最后生成私钥$S_{K_{\mathcal{A}}}$发送给攻击者$\mathcal{A}$。$S_{K_{\mathcal{A}}}=\left\{K_1,K_2,K_3,K_i\right\}_{j\in S}$。

（2）陷门查询。挑战者$\mathcal{C}$随机选择q，运行$\mathrm{Trapdoor}\left(G_{\mathrm{P}},K_S,q\right)\to\left(T_{q_{\mathcal{A}}}\right)$算法，计算$T_1=g^q$、$T_2=\prod_{j=1}^{d}g^{H\left(w_j\right)q}$、$T_3=\prod_{j=1}^{d}g^{H\left(w_j\right)\beta q}$。生成关键字$W$对应的搜索陷门$T_{q_{\mathcal{A}}}=\left\{T_1,T_2,T_3\right\}$发送给攻击者$\mathcal{A}$。

3）挑战。攻击者$\mathcal{A}$向挑战者$\mathcal{C}$发送两个大小相同的关键字w_1、w_2，攻击者$\mathcal{A}$提供访问策略$\left(\boldsymbol{M},\rho\right)$，挑战者$\mathcal{C}$随机选择$b\in\{0,1\}$，生成$w_b$对应的加密关键字索引$I_{w_b}$，随机选择$r\in Z_p^*$，计算$I_1=g^r$、$I_2=g^{\beta r}$、$I_3=g^{\mu r}$，如果关键字包含在文件中，则计算$I_{w_j}=\sum_{j=1}^{d}g^{H\left(w_j\right)\mu r}$，否则$I_{w_j}=1$。挑战者$\mathcal{C}$将$I_{w_b}=\left\{I_1,I_2,I_3,I_{w_j}\right\}$发送给攻击者$\mathcal{A}$。

4）查询阶段2。攻击者$\mathcal{A}$重复进行查询阶段1，查询更多与w_1、w_2不同的关键字集合的搜索陷门。

5）猜测阶段。攻击者$\mathcal{A}$输出b的一个猜想$b'\in\{0,1\}$，若$b'=b$，则攻击者$\mathcal{A}$输出$b'=b$的概率为$\Pr_S\left[b'=b\right]=\frac{1}{2}+\varepsilon$，若$b'\neq b$，则攻击者$\mathcal{A}$输出$b'\neq b$的概率为$\Pr_T\left[b'\neq b\right]=\frac{1}{2}$，因此攻击者$\mathcal{A}$成功的优势如下：

$$A_{\mathrm{dv}}=\left|\frac{1}{2}\Pr_S\left[b'=b\right]+\frac{1}{2}\Pr_T\left[b'=b\right]-\frac{1}{2}\right|=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{4}-\frac{1}{2}=\frac{1}{2}\varepsilon$$

由于攻击者$\mathcal{A}$成功的优势是可忽略的，因此所提方案是安全的，证毕。

4 性能分析

4.1 功能分析

为了证明所提方案的有效性，进行在线/离线加密、策略隐藏、搜索结果排序等方面的比较实验，比较方案选择文献[12-14,19]方案，比较结果如表2所示，其中，√表示具备该功能，×表示不具备该功能。

表2 功能比较

Table 2 Function comparison

方案	在线/离线加密	辅助加/解密	策略隐藏	搜索结果排序
文献[12]方案	×	×	×	×
文献[13]方案	×	×	×	×
文献[14]方案	×	×	√	√
文献[19]方案	×	√	√	×
所提方案	√	√	√	√

由表2可知，除文献[19]方案外的其他方案都支持多关键字搜索，从而提高了方案对文件检索的准确性，特别是文献[14]方案和所提方案可以对搜索后得到的文件进行Top-k排序，但只有所提方案在加密时引入了在线/离线加密机制，因而实现了较低的计算开销。此外，在所提方案中，运用边缘节点辅助解密的设计，密文在被DU解密之前会被EN部分解密，大大减少了DU的计算开销，减轻了客户端负担。文献[19]方案引入外包辅助加/解密的技术，虽降低了客户端的成本，但外包密钥的生成和验证需要额外的开销导致效果不理想。文献[12-13]方案并未实现对访问策略的隐藏，对用户的敏感信息有巨大的安全隐患。相比较而言，所提方案不仅可满足多关键字的密文排序搜索，以及实现策略隐藏和细粒度访问控制，同时与其他方案相比，在降低用户开销方面具有更好的性能。

4.2 计算与存储开销分析

将所提方案与文献[12-14,19]方案在计算、存储开销方面进行对比，结果如表3和表4所示，其中，$\left|G_1\right|$、$\left|G_2\right|$、$\left|Z_p^*\right|$分别表示G_1、G_2、Z_p^*中元素的长度，n_1、n_2分别表示访问策略中的属性个数、与用户相关的属性个数，i表示关键字集中关键字的个数，E_1、E_2表示G_1、G_2上的群指数运算，P表示双线性对运算。

表3　计算开销比较

Table 3　Computational cost comparison

方案	加密	陷门	解密
文献[12]方案	$(2n_1+2)E_1+E_2$	$4E_1$	$2E_2+4P$
文献[13]方案	$(2n_2+5+i)E_1+P$	$(n_2+1)E_1$	$4P$
文献[14]方案	$(4n_1+2)E_1+E_2$	$(n_2+4)E_1$	$2E_1+P$
文献[19]方案	$(6n_1+4)E_1$		$2E_2+2P$
所提方案	$(n_2+3+i)E_1+P$	$3E_1$	E_1+P

表4　存储开销比较

Table 4　Storage cost comparison

方案	密文	密钥
文献[12]方案	$(2n_1+2)\lvert G_1\rvert+\lvert G_2\rvert$	$(n_2+3)\lvert G_1\rvert$
文献[13]方案	$(2n_2+5+i)\lvert G_1\rvert$	$(2n_2+3)\lvert G_1\rvert$
文献[14]方案	$(3n_1+2)\lvert G_1\rvert+\lvert G_2\rvert$	$(2n_2+1)\lvert G_1\rvert$
文献[19]方案	$2n_1\lvert G_1\rvert+(2n_1+6)\lvert G_2\rvert+\lvert G_T\rvert$	$(2n_2+2)\lvert G_1\rvert+6\lvert G_2\rvert$
所提方案	$(4+n_2)\lvert G_1\rvert+\lvert Z_p^*\rvert$	$(5+2n_2+i)\lvert G_1\rvert$

对于计算开销的比较，所提方案在加/解密阶段采用了在线/离线加密技术，与其他方案相比开销较低。对于存储开销的比较，因为云服务器的存储容量不受限，所以所提方案并不考虑云中的密文存储开销。由于用户的密钥长度只与属性相关，因此在所有方案中用户只存储其长度随n_2增加而线性增加的属性。虽然当属性较少时所提方案需要的存储空间较大，但是当属性数随着n_2线性增加时，所提方案的密钥存储开销低于其他方案。以上表明，所提方案在计算和存储开销方面较其他方案有一定优势。

4.3　性能仿真分析

为了更准确地评估方案的实际性能，实验平台配置在Intel® Core™ i5-8250U CPU @ 160 GHz 8.00 GB RAM的笔记本上，基于Java配对加密库（JPBC），采用Type A型素数阶椭圆曲线$y^2=x^3+x$进行仿真实验。为了方便定量分析，假定关键字集中关键字的数量为50，属性数量的取值范围为[10，50]，当属性数量取值为10、20、30、40、50时，各方案在加密和陷门生成阶段的计算时间随属性数量的变化情况分别如图2和图3所示。

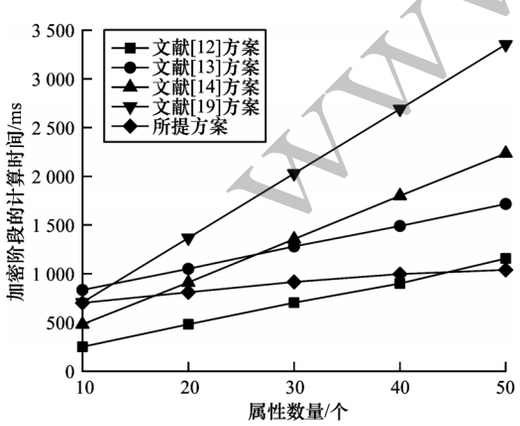

图2　各方案加密阶段的计算时间比较

Fig.2　Comparison of computing time in encryption stage of each scheme

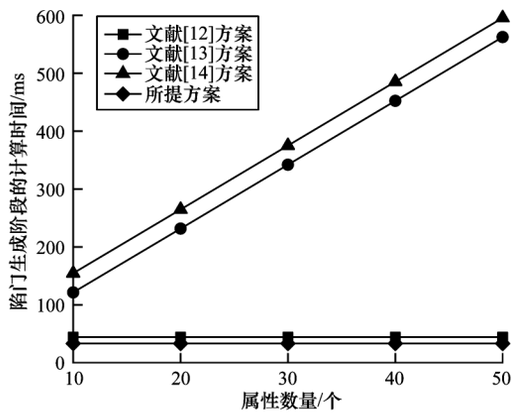

图3　各方案陷门生成阶段的计算时间比较

Fig.3　Comparison of computing time in trapdoor generation stage of each scheme

由图2和图3可知，各方案的加密和陷门生成时间都与属性数量成线性正比关系，所提方案在加密和陷门生成阶段的计算时间相比于次优的文献[12]方案降低了10%和25%。在加密阶段，虽然当属性数量较少时所提方案的计算时间不是最少，但随着属性数量的增加计算时间一直少于其他方案。在陷门生成阶段，与其他方案相比，所提方案的计算时间一直保持在最低的常数级水平。

实验结果分析表明，所提方案不仅实现了高效的多关键字搜索和密文的访问控制，而且具有更好的性能和实用价值。

5　结束语

本文提出云边协同下可排序的属性基可搜索加密方案。采用在线/离线加密和边缘节点辅助计算，在确定访问策略前进行预加密，通过将加密后的数据上传到云端，与其对应的加密索引上传到最近的边缘节点来降低用户的计算负担。将关键字拆分成关键字名和关键字值，用户只能通过公开的关键字名进行匹配，保证了方案安全性。在实现多关键字搜索的情况下对关键字的重要程度进行排序，提高了搜索效率。分析与对比结果表明，所提方案满足IND-CKA安全性，并且与同类方案相比更具高效性。后续将进一步加强所提方案的搜索效率及实用性。

参考文献

[1] AGARWAL K, JHA A K. Intelligence and Internet of Things with 5G technology: application and development [C]//Proceedings of International Conference on Electronics and Renewable Systems. Washington D. C., USA: IEEE Press, 2022: 762-766.

[2] 丁庆丰，李晋国. 一种物联网环境下的分布式异常流量检测方案[J]. 计算机工程，2022，48(8)：152-159.
DING Q F, LI J G. A distributed abnormal traffic detection scheme in Internet of Things environment[J]. Computer Engineering, 2022, 48(8): 152-159. (in Chinese)

[3] 谢娜,谭文安,曹彦,等. 移动边缘计算中安全信息流建模与分析[J]. 计算机工程,2022,48(5):35-42,52.
XIE N,TAN W A,CAO Y,et al. Modeling and analysis of security information flow in mobile edge computing[J]. Computer Engineering, 2022, 48(5): 35-42, 52. (in Chinese)
[4] MCENROE P,WANG S,LIYANAGE M. A survey on the convergence of edge computing and AI for UAVs: opportunities and challenges[J]. IEEE Internet of Things Journal,2022,9(17):15435-15459.
[5] GONG F H. Design of distributed network mass data processing system based on cloud computing technology [C]//Proceedings of the 5th International Conference on I-SMAC(IoT in Social,Mobile,Analytics and Cloud). Washington D. C. ,USA:IEEE Press,2021:1218-1221.
[6] SRIRAM G S. Edge computing vs. cloud computing:an overview of big data challenges and opportunities for large enterprises[J]. International Research Journal of Modernization in Engineering Technology and Science,2022,4(1):1331-1337.
[7] CHANG L Y,ZHANG Z,LI P,et al. 6G-enabled edge AI for metaverse:challenges,methods,and future research directions[J]. Journal of Communications and Information Networks,2022,7(2):107-121.
[8] SONG D X,WAGNER D,PERRIG A. Practical techniques for searches on encrypted data[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C. , USA:IEEE Press,2002:44-55.
[9] MIAO Y B,MA J F,LIU X M,et al. Attribute-based keyword search over hierarchical data in cloud computing[J]. IEEE Transactions on Services Computing, 2020,13(6):985-998.
[10] LI X H,TONG Q Y,ZHAO J W,et al. VRFMS:verifiable ranked fuzzy multi-keyword search over encrypted data[J]. IEEE Transactions on Services Computing,2023,16(1): 698-710.
[11] 闫玺玺,赵强,汤永利,等. 支持灵活访问控制的多关键字搜索加密方案[J]. 西安电子科技大学学报,2022,49(1): 55-66.
YAN X X,ZHAO Q,TANG Y L,et al. Multi-keyword search encryption scheme supporting flexible access control[J]. Journal of Xidian University,2022,49(1):55-66. (in Chinese)
[12] SUN J,REN L L,WANG S P,et al. Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage[J]. IEEE Access,2019,7:66655-66667.
[13] NIU S F,CHEN L X,WANG J F,et al. Electronic health record sharing scheme with searchable attribute-based encryption on blockchain[J]. IEEE Access,2019,8:7195-7204.
[14] SU J,ZHANG L Y,MU Y. BA-RMKABSE:blockchain-aided ranked multi-keyword attribute-based searchable encryption with hiding policy for smart health system[J]. Future Generation Computer Systems,2022,132:299-309.
[15] WU Y L,LI X Y,LIU Z. Attribute-based keyword searchable encryption scheme for multi-authority in cloud storage[C]//Proceedings of the 22nd International Conference on Communication Technology. Washington D. C. ,USA: IEEE Press,2023:933-939.
[16] SUN Y Q,HAN L D,BI J G,et al. Verifiable attribute-based keyword search scheme over encrypted data for personal health records in cloud[J]. Journal of Cloud Computing,2023,12(1):1-13.
[17] VARRI U S,PASUPULETI S K,KADAMBARI K V. Practical verifiable multi-keyword attribute-based searchable signcryption in cloud storage[J]. Journal of Ambient Intelligence and Humanized Computing,2023, 14(9):11455-11467.
[18] MAMTA,GUPTA B B. An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud[J]. Concurrency and Computation: Practice and Experience,2020,32(18):e5291.
[19] ZIEGLER D,MARSALEK A,PALFINGER G. White-box traceable attribute-based encryption with hidden policies and outsourced decryption[C]//Proceedings of the 20th International Conference on Trust,Security and Privacy in Computing and Communications. Washington D. C. ,USA: IEEE Press,2021:331-338.
[20] LING J T,GU H X,WANG H J,et al. An efficient ciphertext index retrieval scheme based on edge computing framework[J]. IEEE Access,2021,9:37975-37988.
[21] TAN X D,CHENG W,HUANG H P,et al. Edge-aided searchable data sharing scheme for IoV in the 5G environment[J]. Journal of Systems Architecture,2023, 136:102834.
[22] DEEBAK B D,MEMON F H,DEV K,et al. AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT[J]. Ad Hoc Networks,2022,125:102740.
[23] 陈虹,侯宇婷,郭鹏飞,等. 可公开验证的高效无证书聚合签密方案[J]. 计算机工程,2022,48(10):146-157.
CHEN H,HOU Y T,GUO P F,et al. Efficient certificateless aggregate signcryption scheme with public verification[J]. Computer Engineering,2022,48(10):146-157. (in Chinese)
[24] MAMTA,GUPTA B B,LI K C,et al. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system[J]. IEEE/CAA Journal of Automatica Sinica,2021,8(12):1877-1890.
[25] YANG X H,ZHANG C S. Blockchain-based multiple authorities attribute-based encryption for EHR access control scheme[J]. Applied Sciences,2022,12(21):10812.
[26] LAN F. Research on text similarity measurement hybrid algorithm with term semantic information and TF-IDF method[EB/OL]. [2023-03-17]. https://www.hindawi.com/journals/am/2022/7923262/.

编辑 陆燕菲