



卫星互联网中层次化多模态数据安全共享方案

郑开发¹, 刘嘉奕², 侯高攀^{3*}, 杨立群⁴, 苗银宾³, 刘志全^{2*}

1. 武汉理工大学信息工程学院, 武汉 430070

2. 暨南大学网络空间安全学院, 广州 511443

3. 西安电子科技大学网络与信息安全学院, 西安 710126

4. 北京航空航天大学网络空间安全学院, 北京 100191

* 通信作者. E-mail: hougapan@xidian.edu.cn, zqliu@vip.qq.com

收稿日期: 2025-11-01; 修回日期: 2026-01-17; 接受日期: 2026-02-13; 网络出版日期: 2026-03-06

国家自然科学基金面上项目 (批准号: 62272195) 和国家自然科学基金青年科学基金项目 (批准号: 62502370) 资助

摘要 随着现代卫星互联网的发展, 敏感多模态数据体量不断增加, 其安全存储与访问面临着极大的挑战. 现有数据共享方案无法兼顾数据搜索效率与搜索过程中的隐私访问控制. 为了解决上述矛盾, 本文提出了一种层次化多模态数据安全共享方案 (SHMDS-SI), 将层次化访问控制与可搜索加密巧妙结合, 实现卫星互联网中多模态数据的安全共享. 首先, 方案选用特异性特征提取方法为异构多模态数据进行特征提取, 输出统一维度的特征向量, 提高数据处理效率; 其次, 方案设计了策略隐藏的属性基加密与可搜索加密算法, 将用户属性嵌入数据密文与查询陷门, 实现安全的密文与搜索过程层次化细粒度访问控制; 最后, 系统通过云边端协同计算协议, 指定用户段的代理服务器协助用户解密, 有效降低了终端设备高昂的计算开销. 本文对方案的安全性进行了严谨的证明. 同时, 理论与仿真分析表明本方案相较现有方案具有更好的搜索效率与性能.

关键词 卫星互联网, 可搜索加密, 多模态数据安全, 属性基加密, 云边端协同计算

1 引言

随着卫星互联网的不断发展, 空间段卫星收集的数据量与数据类型快速增加. 通过各种卫星传感器, 卫星群可以收集文本类型的温度湿度等气象数值化参数^[1]. 低地球轨道 (LEO) 卫星可以利用遥感技术收集大量的图像数据^[2], 还可以在提供通信服务的过程中获取音频类数据^[3]. 因此, 卫星互联网存储处理的数据对象不仅包含单一类型数据, 而且涵盖多种类型的多模态数据. 为了与地面段和用户设备进行安全有效的通信, 需要对隐私多模态数据进行统一化处理与加密操作. 针对以上问题, 特征提取技术已被广泛应用于处理对象为多模态数据的场景. 同时, 可搜索加密 (SE) 技术也为数据的安全访问提供了有效手段. 然而, 目前并无有效解决多模态数据安全高效访问的方案被提出. 另一方面, 卫星互联网中的数据还需根据其机密等级进行细粒度的访问控制, 否则将导致高级机密文件的泄露. 因此, 一种有效结合多模态数据处理, 安全访问与细粒度访问控制的方案是卫星互联网所急需的.

引用格式: 郑开发, 刘嘉奕, 侯高攀, 等. 卫星互联网中层次化多模态数据安全共享方案. 中国科学: 信息科学, 2026, 56: 581–602, doi: 10.1360/SSI-2025-0465

Zheng K F, Liu J Y, Hou G P, et al. Secure hierarchical multi-modal data sharing scheme in satellite Internet. Sci Sin Inform, 2026, 56: 581–602, doi: 10.1360/SSI-2025-0465

多模态数据因其跨模态的特点, 表达方式与传输格式各不相同. 而通过数据特征提取的方式可以将其转化为表达方式统一的向量形式, 极大降低了后续处理数据的难度. 在多模态数据处理工作中, 深度学习因其强大的表征学习能力被广泛应用^[4~6]. 卷积神经网络 (CNNs) 在图像特征提取方面表现出色, 能够捕捉局部感受野内的空间和通道信息, 输出较为准确的特征向量^[7]. 循环神经网络 (RNNs) 与 Transformer 模型则在处理文本等序列数据方面具有优势^[6,8]. 尽管当前已对多模态数据特征提取的技术进行了深入的研究, 但仍缺少相关文献对多模态数据进行规范的特异性提取.

针对多用户场景下的数据搜索与通信, 数据隐私性对数据的安全访问与细粒度访问控制具有极高要求. 可搜索加密 (SE) 方案^[9] 的提出为数据安全访问提供了有效的技术手段, 其通过独特的加密方式, 确保数据在加密状态下可以实现准确的检索与访问. 但仅通过可搜索加密技术对卫星互联网的层次性机密数据进行加密远远不够, 还需要对用户访问的权限进行细粒度控制. 属性基加密 (ABE), 一种嵌入用户属性特征进行加密的技术, 可以有效解决隐私数据的细粒度访问控制. ABE 方案一般分为基于密文策略 (CP)^[10] 以及基于密钥策略 (KP)^[11] 的属性基加密. CP-ABE 方案的密文与访问结构相关, 数据访问控制更灵活, 因此相较 KP-ABE 使用更广泛. 然而, 目前将 SE 与 ABE 相结合的方案^[12,13] 一般将用户属性嵌入密文处, 单独设计查询陷门, 增加了密文的复杂性.

传统的集中云处理方式会导致网络的拥塞和延时^[14], 降低用户段终端设备的体验. 由于卫星互联网用户段中多为移动终端设备, 其计算资源有限, 需要边缘服务器协助计算. 然而, 边缘服务器作为半可信机构, 会尝试对接触到的数据进行破解. 这对加密数据的隐私性提出了很高的要求. 文献 [15,16] 引入雾计算, 在保证安全性的前提下, 通过将部分终端设备开销转移至雾节点降低其计算开销. 但是以上方案均不能被通用性地应用至卫星互联网系统中.

针对现有方案在多模态特征提取与协同计算架构方面的不足, 本文提出一种面向卫星互联网的云边端协同属性基可搜索加密方案. 为适应星上算力与能耗受限的约束, 数据所有者仅执行轻量初始加密, 将计算密集的二次加密卸载至地面代理服务器, 从而降低板载计算负载. 面向星地链路带宽受限问题, 方案通过特异性特征提取将多模态数据统一为特征向量并构建轻量索引. 进一步地, 考虑卫星网络高时延与间歇连接特性, 构建具备计算中继与缓存能力的协同架构, 使用户在覆盖盲区仍可经地面网络获取预处理解密参数, 降低对卫星实时的依赖, 并在隐私保护与细粒度访问控制前提下实现高效共享. 本文的创新点与贡献如下所示.

(1) 创新的多模态敏感数据特征提取方法: 为解决多模态数据异构格式的问题, 方案选用特异性的特征提取方式提取各模态数据特征, 并输出相同维度的特征向量, 使得数据表达方式统一化, 提高后续数据处理的效率和方案的扩展性.

(2) 支持层次化的策略隐藏的高安全搜索算法: 考虑卫星互联网数据的层级机密性, 基于策略隐藏设计分层访问控制机制, 提高系统安全性. 同时, 将用户属性作为搜索令牌嵌入查询陷门中, 实现了搜索过程中的细粒度访问控制, 提高了数据访问的灵活性与隐私性.

(3) 支持云边端协同的敏感数据共享算法: 为降低用户段移动终端设备的计算开销, 设计云边端协同计算协议. 在保证隐私性和安全性前提下, 将地面段的代理服务器分配给终端设备协助解密, 有效转移了数据解密过程的计算开销, 提高了用户段设备体验与计算效率.

2 相关性工作

在卫星互联网体系中, 空间段的卫星可以收集图像、音频、文本等多模态数据. 为了解决海量数据的安全存储与隐私访问, 学者此前已将可搜索加密技术应用于物联网系统^[17]、医疗数据管理^[18] 等领域. 相似地, 本文将可搜索加密技术应用于卫星互联网系统中. 此外, 我们在可搜索加密基础上结合属性基以及云边端协同计算架构, 实现多模态数据隐私访问. 学者对多模态数据处理, 属性基可搜索加密方案与云边端协同计算架构等方面的已有研究对本文方案的提出奠定了基础.

多模态数据包含多种不同表达方式的数据类型, 其跨模态的特性使数据处理极为不便. 因此, 学者对多模态

数据进行特征提取并输出统一维度的特征向量^[19],有效整合了异构数据源,为后续的加密及搜索操作奠定基础. Xu等^[20]提出了一种多模态量化混合机制(MMQ),构造了一个双阶段框架用于训练一种新的多模态标记器.该方案采用正交正则化方法捕获多模态信息,并根据下游推荐目标动态调整语义,有效统一了多模态数据的协调性和行为适应性.然而,该方案对于资源有限的终端移动设备而言过于复杂.此外,学者基于特征提取提出了多模态数据融合方法,基于数据权重对跨模态数据进行融合,获得比单一模态数据更全面的数据表示. Zhang等^[21]提出了一种基于注意力机制的深度多模态融合网络.在注意力模型中,方案采用分层融合方法确保多模态融合的有效性,并根据数据的重要性自动分配每个模态的融合比例,有效地提高了数据利用的准确性.

云环境下数据的安全搜索与细粒度访问控制难题制约了隐私数据的安全性.在 Bethencourt等^[10]提出了基于密文策略的属性基加密(CP-ABE)方案以及 Song等^[9]提出了可搜索加密(SE)方案后,上述难题迎刃而解.此后,学者针对属性基加密以及可搜索加密进行了深入的研究,出现了巧妙结合属性基加密与可搜索加密技术的属性基可搜索加密(ABSE)方案. Yin等^[22]基于上述思想提出了一种去中心化的基于密文策略的可搜索属性基加密方案.该方案结合基于属性的可搜索加密技术的研究,提高隐私医疗保健数据在云服务器中的安全性.此外,该方案通过引入区块链的属性节点,有效避免了单点故障的问题.然而,区块链的引入意味着更大的资源消耗以及部署难度,无法在涉及范围广泛的卫星互联网系统有效部署. Mamta等^[23]构造了一种属性基可搜索加密的高效密钥策略设计框架.在基础的ABSE方案基础上添加了用户的可撤销功能,提高了多用户场景下的可用性.但其搜索过程并未与用户属性相结合,可能导致恶意攻击者伪造身份搜索机密信息.

由于卫星互联网中用户段大多由资源有限的移动终端设备组成,实现轻量级的终端计算对系统运行效率有重要的意义.因此,学者对云边端协同计算架构进行了广泛研究. Zheng等^[12]在云环境中提出了一种支持云边端协同计算的多关键词密文检索方案.该方案通过加入边缘服务器计算,将用户的加解密计算开销通过预加密等方式转移至边缘服务器处,极大减少了终端用户的计算开销,提高了计算效率与用户体验.然而,该云计算架构设计方式过多依赖边缘服务器实现有效的加解密过程.若边缘服务器出现故障或脱离系统,将导致系统完全无法运行,风险较高.

3 基础知识

3.1 卫星通信网络基本架构

一个基本的卫星互联网系统通常包括空间段、地面段以及用户段^[24].其中空间段由多颗卫星组成,根据轨道离地高度,可以将其分为地球静止轨道卫星(GEO)、地球轨道卫星(MEO)和低地球轨道卫星(LEO).空间段负责数据的接收、处理与转发,并与地面段通信.地面段由控制中心、边缘服务器及基站等组成,负责数据存储与处理,同时作为中枢协调空间段与用户段的通信.用户段主要为大量的用户终端,包括各种移动设备、物联网设备等,这些设备需要接收空间段收集的多模态数据进行工作.

除了上述基础组成部分外,现代卫星互联网中还引入了空中段,通常为无人机等空中作业设备.在地面基础设施不足的地区,空中段可以提供短时通信,连接空间段与地面段.图1为卫星互联网的基本架构图.

3.2 双线性映射

假设 G 与 G_T 为两个阶为大素数 p 的乘法循环群,从群 G 中挑选一个生成元 g .我们定义 $e: G \times G \rightarrow G_T$ 为一个双线性映射函数,函数输入两个群 G 中的元素并输出一个群 G_T 中的元素.上述双线性映射函数具有如下性质.

- (1) 双线性: 对于任意元素 $u, v \in G, a, b \in \mathbb{Z}_p^*$, 满足 $e(u^a, v^b) = e(u, v)^{ab}$.
- (2) 非退化性: 存在 $a, b \in \mathbb{Z}_p^*$, 使得 $e(g^a, g^b) \neq 1$.
- (3) 可计算性: 对于任意元素 $u, v \in G$, 存在有效的算法计算 $e(u, v)$ 的值.

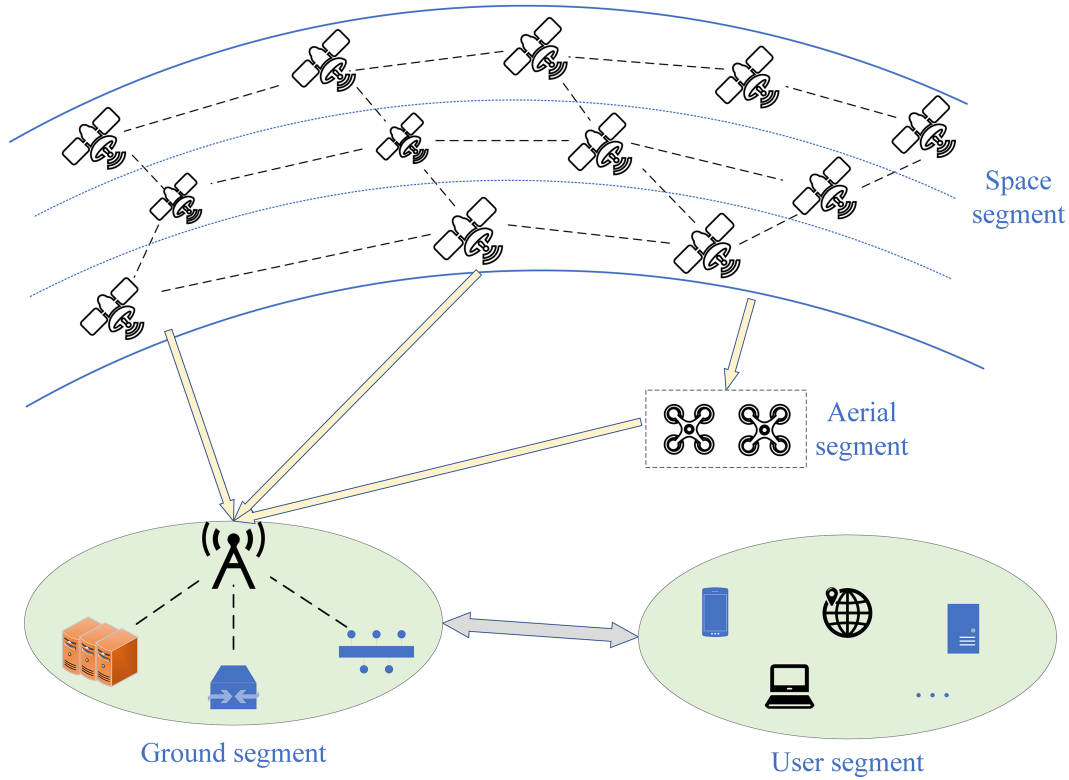


图 1 (网络版彩图) 卫星互联网架构图.

Figure 1 (Color online) Architecture of satellite Internet.

3.3 决策性双线性 Diffie-Hellman (DBDH) 假设

$e: G \times G \rightarrow G_T$ 为一个双线性映射函数. 随机挑选生成元 $g \in G$, 以及随机数 $a, b, c \in \mathbb{Z}_p^*$. 多项式时间敌手 $\mathcal{A}$ 可以获得参数 $(g, g^a, g^b, g^c, e(g, g)^{abc}, T \in G_T)$, 其中 T 为群 G_T 中的随机元素. DBDH 问题定义为: 敌手 $\mathcal{A}$ 根据已有参数判断随机元素 T 是否与 $e(g, g)^{abc}$ 相等. 若相等, $\mathcal{A}$ 输出 1; 否则, 输出 0.

我们定义 $\mathcal{A}$ 解决上述问题的优势为

$$Adv = |Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - Pr[\mathcal{A}(g, g^a, g^b, g^c, T) = 1]|. \quad (1)$$

若不存在多项式敌手 $\mathcal{A}$, 可以以不可忽略的优势解决 DBDH 问题, 则 DBDH 假设在群 G, G_T 中成立.

4 系统模型

4.1 系统架构

本文所讨论的卫星互联网系统中所涉及的设备可总结为 5 类实体, 分别为数据拥有者 (data owners, DOs)、数据用户 (data users, DUs)、云服务提供商 (cloud service provider, CSP)、代理服务器 (proxy servers, PSs) 以及密钥生成中心 (key generation center, KGC). 通过实体间的相互通信以及数据处理, 空间段的卫星所收集的多模态数据得以安全高效地被用户段的用户使用. 图 2 为 SHMDS-SI 方案的实体交互架构图, 下文将对 5 类实体的构成以及具体功能进行介绍.

(1) 数据拥有者 DOs: 为空间段的各类卫星, 负责收集多模态数据并根据数据机密层级进行分层. DOs 还会进行简单的数据加密操作, 与地面层通信, 将初始密文传输至地面段.

(2) 数据用户 DUs: 为用户段的各种终端设备, 具有获取数据的需求. 其会构造查询陷门通过 PSs 向 CSP 进行数据查询, 并进行轻量级的解密操作获取所需的多模态数据.

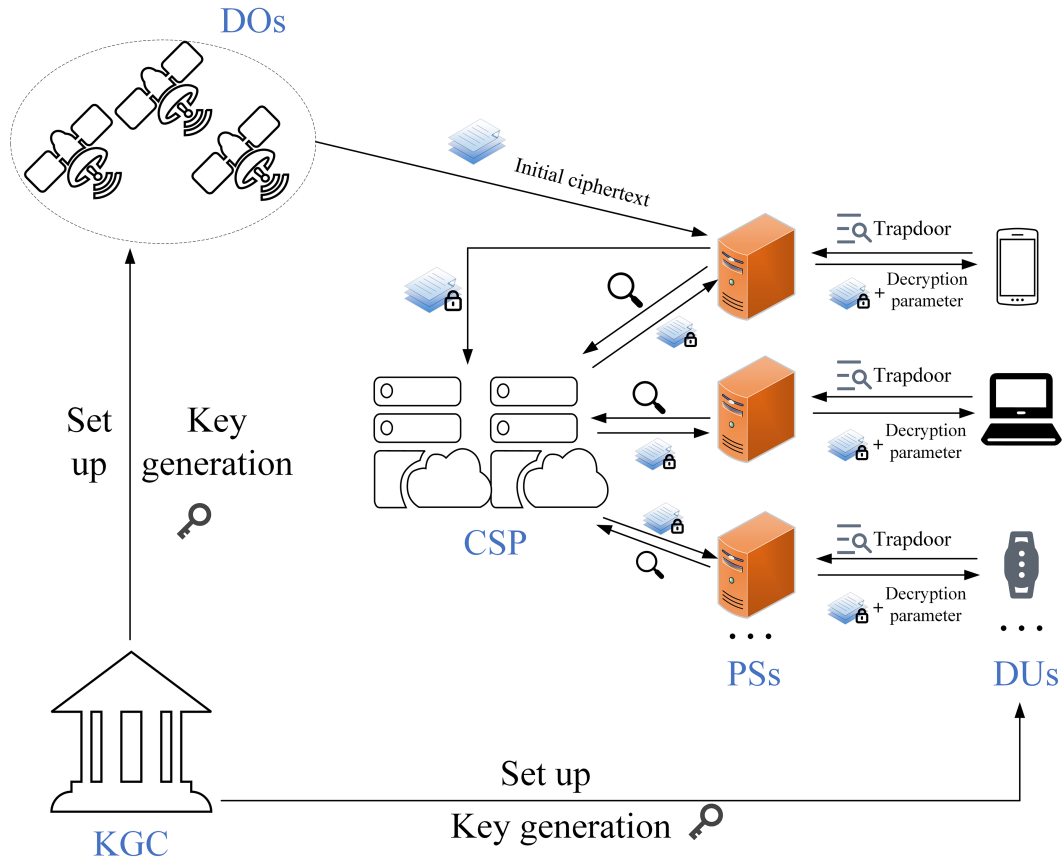


图 2 (网络版彩图) 实体交互架构图.

Figure 2 (Color online) Architecture diagram of entity interaction.

(3) 云服务提供商 CSP: 位于地面段的半可信机构, 由具备强大存储计算能力的服务器组成. 负责存储 PSs 发送的密文以及 DOs 发送的索引, 并根据 DUs 提供的查询陷门进行数据匹配搜索.

(4) 代理服务器 PSs: 位于地面段的半可信机构, 具备一定的数据处理与存储能力. PSs 可以接收 DOs 的初始密文并进行二次加密. 在每个 DU 的上游均对应一个代理服务器 PS, 负责接收 DUs 传来的查询陷门并返回 CSP 的搜索结果, 为 DUs 计算解密参数.

(5) 密钥生成中心 KGC: 位于地面段的可信机构, 负责进行系统的初始化以及公共参数、秘密参数的生成. 其为各实体分发公私钥对, 并管理所有的实体私钥与秘密参数.

此外, 在这 5 类实体中, 数据用户 DUs、云服务提供商 CSP 以及代理服务器 PSs 均可能成为威胁系统安全的潜在敌手. DUs 的访问权限各不相同, 不具备权限的用户可能通过进行超限询问尝试以及密文截取来获取敏感信息. CSP 与 PSs 均为半可信机构, 即能够保证完成方案所设定的任务, 但会凭借自身可接触到的加密数据, 包括密文、加密索引、查询陷门等内容推测破解敏感明文信息.

基于上述实体模型, 下面以卫星互联网中的典型应用场景说明本文方案的实用性. 在森林火灾应急响应中, 空间段的遥感卫星 (DO) 拍摄到某区域的森林火灾红外图像 (图像模态) 及定位数据 (文本模态). DO 首先提取灾情特征向量, 对多模态数据执行初始加密并回传至地面站 (PSs). 地面指挥中心的用户 (DU, 如消防指挥官) 持有包含“绝密权限”及“应急部门”等属性的私钥, 并生成包含“火灾”关键词的搜索陷门发送至云端 (CSP). CSP 在不解密的情况下匹配出相关影像索引. 最后, 代理服务器 (PSs) 协助指挥官的移动终端完成解密, 使其能快速获取火场态势信息. 该流程完整体现了从多模态采集、隐私保护检索到分级授权访问的闭环.

表 1 符号描述.

Table 1 Notation description.

Notation	Description
$\mathcal{D}_L$	Multi-modal data of classification level l
$\vec{v}_L$	Feature vector extracted from $\mathcal{D}_{(l)}$
msk	Secret parameter
pp	Public parameter
(pk, sk)	Public-private key pair of entity
id	Classification level marking
Tok	Search token
SK	Attribute key
C	Multi-modal data ciphertext
I	Data index
T	Trapdoor
$\hat{C}$	Search result ciphertext

4.2 方案形式化定义

SHMDS-SI 方案共包含 6 个主要算法, 即初始化 *Setup*、密钥生成 *KeyGen*、数据加密 *Encrypt*、加密索引生成 *IndexBuild*、用户搜索 *Search*, 以及数据解密 *Decrypt*. 表 1 给出了文中主要符号的描述, 下文将对算法进行形式化定义.

(1) 初始化 $Setup(1^\mu) \rightarrow (msk, pp)$: KGC 输入安全参数 μ , 输出秘密参数 msk 与公共参数 pp .

(2) 密钥生成 $KeyGen(msk, pp, S_{DU}) \rightarrow ((pk, sk), Tok, id, SK)$: KGC 输入秘密参数 msk 以及公共参数 pp , 为实体 DOs 和 DUs 生成私钥 sk , 并计算对应公钥 pk , 为 DUs 生成属性密钥 SK . 此外, KGC 为每一个机密层级设置唯一的随机数, 并计算对应标识 id 与搜索令牌 Tok .

(3) 数据加密 $Encrypt(\mathcal{D}_L, pp, pk) \rightarrow C$: DOs 输入多模态数据明文 $\mathcal{D}_L$ 以及公共参数 pp , 将其加密为初始密文 C_0 并传输给 PS. PS 进行密文二次加密, 输出最终密文 C .

(4) 加密索引生成 $IndexBuild(id, \vec{v}_L, pp, pk) \rightarrow I$: DOs 输入特征向量 $\vec{v}_L$ 以及层级标识 id , 输出加密索引 I 并传输至 CSP.

(5) 用户搜索 $Search(\mathcal{D}_q, Tok, I, sk) \rightarrow \hat{C}$: 首先, DUs 输入查询数据 $\mathcal{D}_q$ 、搜索令牌 Tok 以及用户私钥 sk_{DU} , 输出查询陷门 T 并传输至上游 PS 处. 接着, 由 PS 向 CSP 提出查询请求, CSP 输入查询陷门 T 和索引 I , 输出结果密文 $\hat{C}$, 返回给 PS.

(6) 数据解密 $Decrypt(\hat{C}, SK) \rightarrow \hat{\mathcal{D}}$: PS 为 DU 计算解密参数 par 并将其与结果密文 $\hat{C}$ 一同传输至 DU 处. DU 输入属性密钥 SK , 解密参数 par 与结果密文 $\hat{C}$, 经过轻量级解密计算输出多模态数据明文 $\hat{\mathcal{D}}$.

4.3 安全目标

为了明确 4.1 小节中指出的系统潜在敌手的解决方案, 本节将对方案的安全目标进行详细说明. 本文将会针对安全目标设计安全高效的多模态数据共享方案.

(1) 层次化数据共享机制可靠性: 需要设计一种面向多模态数据的层次化安全共享机制. 要求对于不同权限的数据用户 DUs, 能够分发满足其权限的查询令牌, 实现数据的安全访问. 防止不具备权限的用户通过超限查询尝试或截取查询信息获得敏感信息.

(2) 数据加密方案安全性: 需要设计一种安全的数据加密方案对敏感明文数据进行加密, 确保密文的不可区分性. 即使半可信机构拥有任意密文数据, 也无法借此获取任何敏感信息.

(3) 数据搜索机制隐私性: 需要一种安全的加密索引和查询陷门构造方式, 确保加密索引、查询陷门的隐私

性以及查询陷门的不可链接性. 即使半可信机构拥有由敏感数据构造的索引和查询陷门, 也无法获取敏感明文信息.

4.4 安全模型

定义1 选择明文攻击 (CPA): 敌手 $\mathcal{A}$ 可以任意选择明文并通过一个加密机获取其对应的密文. 敌手 $\mathcal{A}$ 的目标是通过已知明文密文对, 尝试破解密文间的不可区分性.

定理1 在 DBDH 假设成立的前提下, 只有当不存在敌手 $\mathcal{A}$ 可以在概率多项式时间 (PPT) 内以不可忽略的优势 ϵ 赢得下述游戏时, 该方案被认为是 CPA 安全的.

初始化: 挑战者 $Chal$ 运行初始化算法 $Setup$, 输出秘密参数 msk 与公共参数 pp . $Chal$ 保留 msk , 并将 pp 交给敌手 $\mathcal{A}$.

阶段 1: 敌手 $\mathcal{A}$ 任意挑选明文 M 并查询其对应密文. 挑战者 $Chal$ 运行加密算法 $Encrypt$, 输出密文 C^* 并返回给敌手 $\mathcal{A}$.

挑战: 敌手 $\mathcal{A}$ 挑选两个等长的明文消息 M_0, M_1 , 并将其提交给 $Chal$. $Chal$ 随机选择 $b \in \{0, 1\}$, 计算密文 C_b 并将其发给敌手 $\mathcal{A}$.

阶段 2: 询问方式与阶段 1 相同, 但是消息 M_0, M_1 不能被重复查询.

猜测: 敌手 $\mathcal{A}$ 基于已知的明文密文对进行猜测, 输出 $b' \in \{0, 1\}$. 如果 $b' = b$, 敌手 $\mathcal{A}$ 赢得该游戏; 否则敌手 $\mathcal{A}$ 失败.

我们定义敌手 $\mathcal{A}$ 获胜的概率为

$$Pr = \left| Pr(b' = b) - \frac{1}{2} \right|. \quad (2)$$

5 方案实施

5.1 多模态数据特征提取

庞大的卫星互联网可以收集海量的数据资源, 其中包含文本、图片影像、音频等多模态数据. 为了统一多模态数据的形式, 方便进行数据的统一化处理, 本方案对不同模态的数据采用相应方式提取特征, 得到相同维度的特征向量. 本节将介绍对不同模态数据的统一化处理方式.

对于输入的多模态数据元组 $\mathcal{D} = \{D_t, D_i, D_a\}$, 其中 D_t, D_i, D_a 分别对应文本、图像、音频数据, 我们采取以下特征提取方式获得对应的不同维度特征向量, 提取网络结构如图 3 所示.

- 文本: $\vec{v}_t = BERT(D_t) \in \mathbb{R}^{m_t}$.
- 图像: $\vec{v}_i = ResNet(D_i) \in \mathbb{R}^{m_i}$.
- 音频: $\vec{v}_a = Wav2Vec(D_a) \in \mathbb{R}^{m_a}$.

本方案采用 BERT-Base (bidirectional encoder representations from transformers) 模型提取文本特征. 该模型由 12 层 Transformer Encoder 堆叠而成, 利用多头自注意力机制捕获长距离依赖关系. 对于数据集给定的输入文本序列 $S = \{w_1, w_2, \dots, w_n\}$, 首先通过 WordPiece 分词器进行切分, 并在句首插入分类标记 [CLS], 句尾插入分隔标记 [SEP]. 在第 l 层编码器中, 输入向量 H^{l-1} , 通过 3 个线性投影矩阵 W_Q, W_K, W_V 生成查询、键和值矩阵. 注意力输出计算如下:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V, \quad (3)$$

其中 $\sqrt{d_k}$ 为缩放因子. 经过 12 层编码后, 提取 [CLS] 标记对应的最后一层隐藏状态 $h_{[CLS]}$, 即文本特征向量 $\vec{v}_t \in \mathbb{R}^{m_t}$.

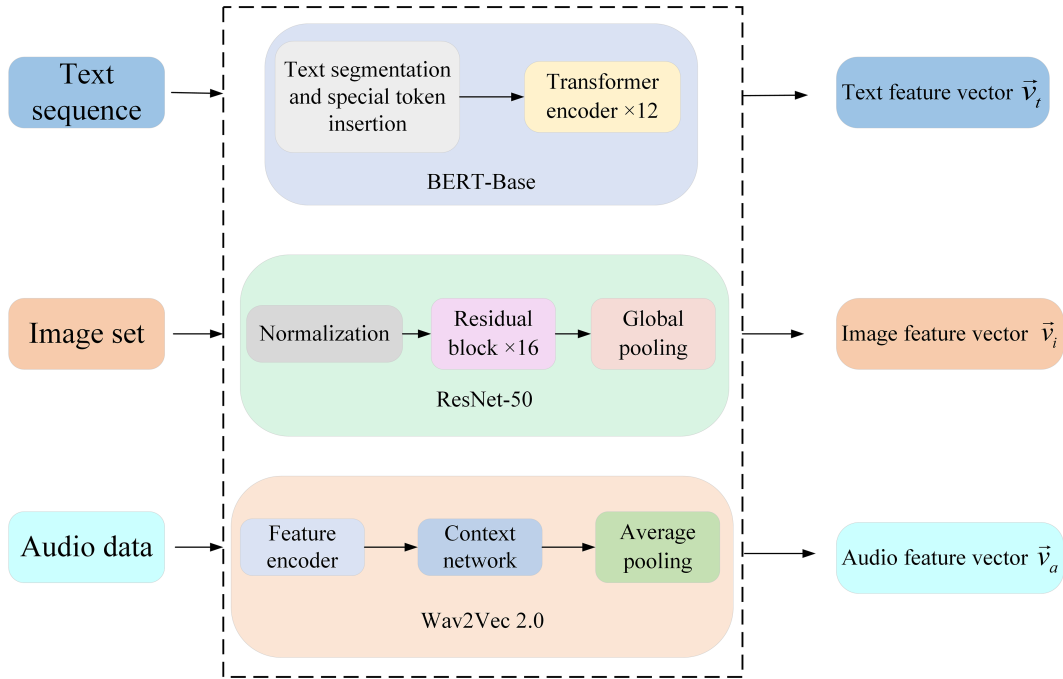


图3 (网络版彩图) 多模态数据特征提取网络结构图.

Figure 3 (Color online) Multi-modal data feature extraction network structure diagram.

为了提取图像的深层视觉语义, 本方案采用 ResNet-50 架构. 所有输入图像通过预处理调整为 $224 \times 224 \times 3$ 的标准尺寸. 网络核心由 16 个“瓶颈”残差块组成, 每个块包含 $1 \times 3, 3 \times 3, 1 \times 1$ 三个卷积层. 对于输入 x , 残差块的输出定义为 $F(x) + x$, 其中 $F(x)$ 为残差映射. 本方案移除了全连接分类层, 并应用全局平均池化操作, 在不破坏空间结构信息的前提下获取固定长度的特征向量.

$$\vec{v}_i = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W \text{featuremap}(i, j), \quad (4)$$

其中 H 为 feature map 的高度, W 为 feature map 的宽度. 最终得到图像特征向量 $\vec{v}_i \in \mathbb{R}^{m_i}$.

针对音频数据的时序性和连续性, 本方案采用 Wav2Vec 2.0 模型. 将原始音频重采样为 16 kHz, 输入为一维波形向量. 模型主要包含三个模块: 特征编码器、上下文网络与时序池化. 特征编码器由 7 层一维卷积神经网络组成, 将原始音频波形 $\mathcal{X}$ 降采样并编码为潜在语音表示 $\mathcal{Z} = z_1, \dots, z_T$. 上下文网络采用 Transformer 架构, 将潜在表示 $\mathcal{Z}$ 转换为包含上下文信息的表示 $\mathcal{C} = c_1, \dots, c_T$. 由于 Transformer 输出的是帧级别的特征序列, 最后对所有时间步的上下文向量进行平均池化, 得到定长的音频特征向量 $\vec{v}_a \in \mathbb{R}^{m_a}$.

为了将上文提取出的不同维度的多模态特征向量进行维度对齐, 本方案在特征提取网络的末端进行特征对齐, 采用特征向量拼接的策略实现多模态特征的融合与维度对齐. 特征对齐操作将三种模态的特征向量按顺序进行串联, 构建一个统一维度的多模态融合特征向量 $\vec{v}$. 特征对齐流程如图 4 所示.

$$\vec{v} = \text{Concat}(\vec{v}_t, \vec{v}_i, \vec{v}_a) \in \mathbb{R}^m, \quad (5)$$

其中 $m = m_t + m_i + m_a$. 通过上述特征提取过程, 跨模态的数据类型被统一为 m 维的特征向量 $\vec{v}$. 特征向量维度 m 是平衡检索精度、方案安全性以及系统开销的关键参数. 首先, m 决定了特征空间的容量, 过小的 m 会导致数据特征的丢失, 增加碰撞的概率, 从而降低搜索精确率. 根据本方案关于准确率的实验结果, 当 $m > 128$ 时, 可以保证较高的精确率. 其次, 根据式 (11), m 与加密索引相关, 较大的 m 可以扩大 $\sum_{i=1}^m \vec{v}_L^{(L)}$ 的值, 增强方案抗特征猜测攻击的能力. 根据性能分析部分的实验结果, 方案的计算开销与 m 呈正相关, 若为了检索精度与安

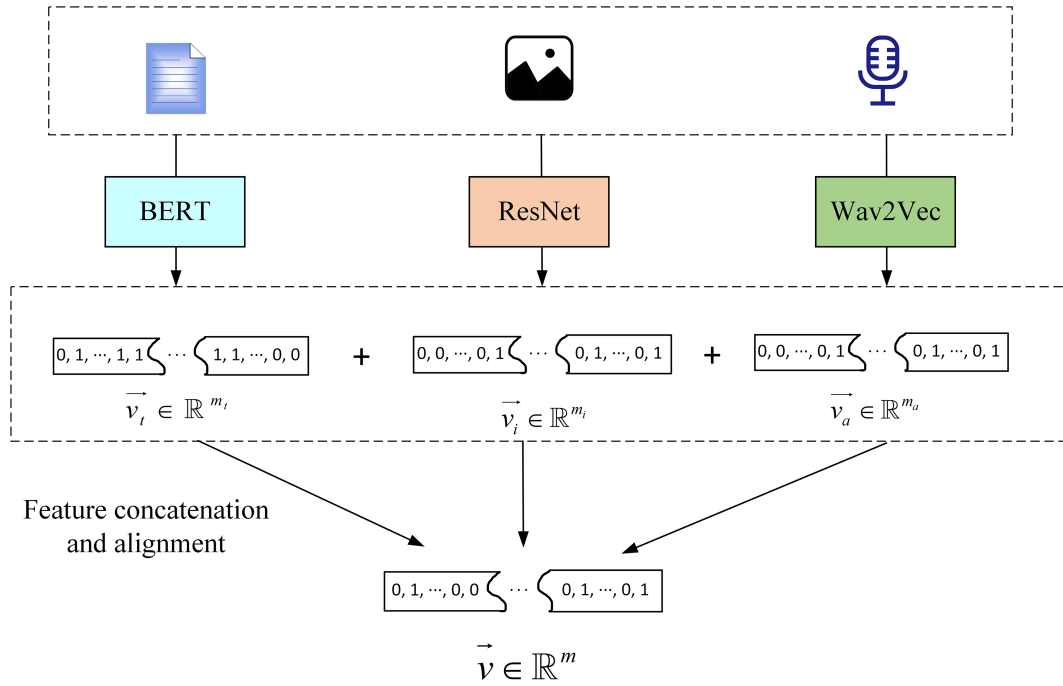


图4 (网络版彩图) 特征对齐流程图.

Figure 4 (Color online) Feature alignment flow diagram.

全性过度增加 m 的大小, 会导致计算开销超过地面段与空间段用户的资源上限. 因此, 考虑到卫星互联网有限的计算资源, 本文选取 $m = 512$.

本方案要求空间段卫星与用户段终端设备借助上述多模态特征提取网络进行特征提取, 而模型训练需要消耗大量的算力与资源, 无法在资源有限的卫星与终端实现. 因此, 本方案设计将训练完成的模型通过预先上传的方式交付给卫星与终端设备, 在系统运行时, 只需进行轻量级的前向推理即可得到特征向量, 实现了特征提取的可行性与开销的降低.

5.2 主要算法

SHMDS-SI 方案共 6 个主要算法, 包括初始化 *Setup*、密钥生成 *KeyGen*、数据加密 *Encrypt*、加密索引生成 *IndexBuild*、用户搜索 *Search*, 以及数据解密 *Decrypt*.

卫星互联网中储存的数据丰富, 其中包括涉及国家机密的隐私数据. 为了保护隐私数据的安全性, 空间段的卫星将传输的数据根据机密层级进行分层处理. 为便于描述, 本文仅对第 L 层的数据进行讨论, 即 $\mathcal{D}_L$. 假设系统属性集为 $\mathbb{S} = \{att_1, att_2, \dots, att_n\}$, 我们根据数据用户 DUs 的权限为每一个 DU 设置用户属性集 $S_{DU} \in \mathbb{S}$. 图 5 为算法流程图, 下面是算法的具体描述.

(1) 初始化 $Setup(1^\mu) \rightarrow (msk, pp)$. 密钥生成中心 KGC 输入安全参数 μ , 输出秘密参数 msk 以及公共参数 pp .

$$\begin{cases} msk = \{\beta, \xi, \{V_{att_i}\}_{att_i \in \mathbb{S}}, \{s_j\}_{j \in [1, n]}\}, \\ pp = \{G, p, e, g, h, g^\beta, g^\xi, \{g^{s_j}\}_{j \in [1, n]}\}. \end{cases} \quad (6)$$

在秘密参数 msk 中, β 为群 $\mathbb{Z}_p^*$ 中的随机元素. 在公共参数 pp 中, G 是一个阶为大素数 p 的乘法循环群, e 为一个双线性映射函数. g, h 为群 G 的两个生成元. 对于每个属性 att_i , KGC 设置唯一值 V_{att_i} 与其对应, 生成属性值集合 $\{V_{att_i}\}_{att_i \in \mathbb{S}}$. 同时, KGC 为每个系统属性分配一个秘密值, 生成属性秘密值集合 $\{s_j\}_{j \in [1, n]}$.

(2) 密钥生成 $KeyGen(msk, pp, S_{DU}) \rightarrow ((pk, sk), Tok, id, SK)$. KGC 输入秘密参数 msk 以及公共参数 pp , 为卫星 (即数据拥有者 DO) 和具备访问第 L 层数据权限的用户 DU 生成各自的公私钥对.

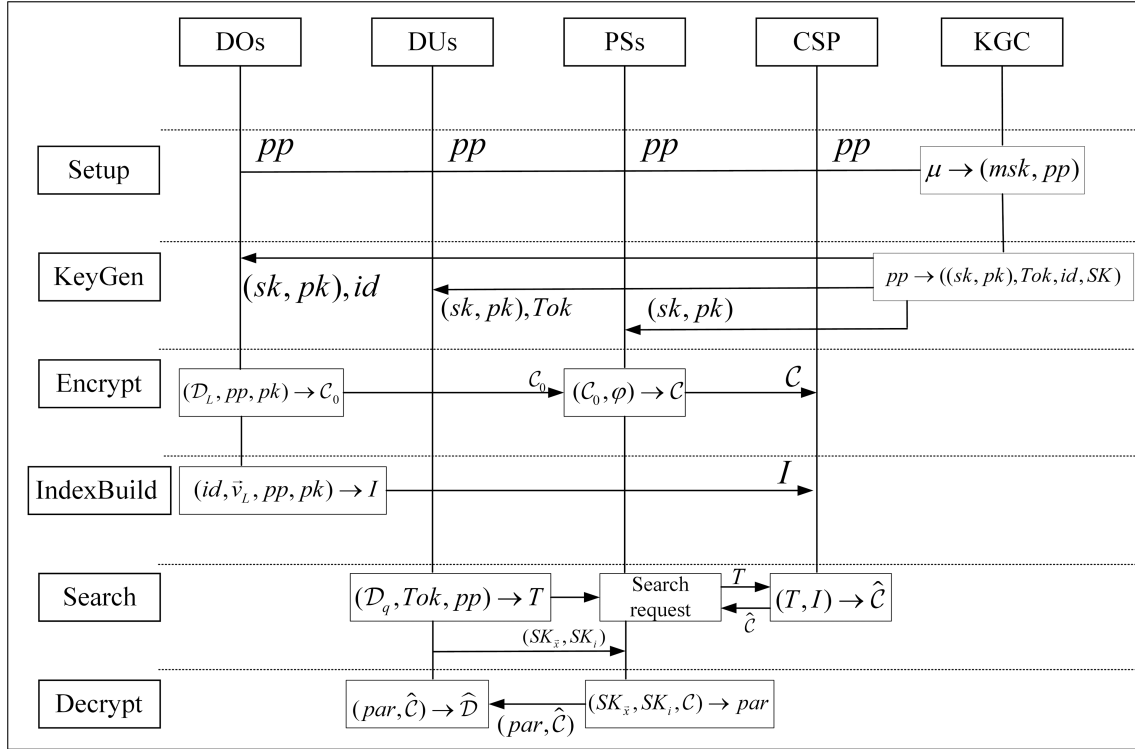


图 5 算法流程图.

Figure 5 Algorithm flow diagram.

- DO: 生成密钥 $sk_{DO} = r \in \mathbb{Z}_p^*$, 并计算对应公钥 $pk_{DO} = g^r$.
- DU: 生成密钥 $sk_{DU} = p \in \mathbb{Z}_p^*$, 并计算对应公钥 $pk_{DU} = g^p$.

随后, KGC 为机密层级 L 分配一个唯一的随机数 λ . 假设符合该机密层级访问策略的用户 DU 的属性集为 $S_{DU} = \{att_1, att_2, \dots, att_L\}$, 满足 $\lambda = \sum_{att_i \in S_{DU}} V_{att_i}$. KGC 为数据所有者 DO 计算用于加密索引生成的层级标识 $id = g^\lambda$, 为用户 DU 计算搜索令牌 $Tok = \{h^{V_{att_i}}\}_{att_i \in S_{DU}}$.

对于符合第 L 层访问策略的用户 DU, KGC 首先为其生成属性向量 $\vec{x}$, 对系统属性集 $\mathbb{S}$ 中的每一个属性 att_i , 如果 $att_i \in S_{DU}$, 则令 $x_i = V_{att_i}$, 否则 $x_i = 0$, 如式 (7) 所示:

$$x_i = \begin{cases} V_{att_i}, & att_i \in \mathbb{S}, \\ 0, & att_i \notin \mathbb{S}. \end{cases} \quad (7)$$

那么对于用户 DU, 可以生成属性向量 $\vec{x} = \{V_{att_1}, V_{att_2}, \dots, V_{att_L}, 0, \dots, 0\}$. 在生成属性向量 $\vec{x}$ 后, KGC 为 DU 计算属性密钥 SK , 如式 (8) 所示:

$$SK = \{SK_0 = g^{\lambda \cdot \xi}, SK_{\vec{x}} = g^{\lambda(\sum_{i=1}^n s_i \cdot x_i + \xi) + \beta}, SK_i = g^{\lambda \cdot x_i}, i \in [1, n]\}. \quad (8)$$

算法运行完成后, KGC 将生成的私钥 sk 发送给对应实体, 并公开所有公钥 pk , 将标识 id 发送给 DO, 将搜索令牌 Tok 以及属性密钥 SK 发送给 DU.

(3) 数据加密 $Encrypt(\mathcal{D}_L, pp, pk) \rightarrow \mathcal{C}$. 该算法由 DO 以及 PS 共同运行完成. DO 根据指定的访问策略 $\Gamma \in \mathbb{S}$ 生成策略向量 $\vec{y}$, 满足 $\vec{x} \cdot \vec{y} = 0$.

首先, DO 输入多模态数据 $\mathcal{D}_L$, 进行初始密文计算. DO 为数据 $\mathcal{D}_L$ 挑选一个随机元素 $d \in \mathbb{Z}_p^*$ 并计算如式 (9) 所示的初始密文.

$$\mathcal{C}_0 = (c'_D = \mathcal{D}_L \cdot e(g, g)^{\beta \cdot d}, c' = g^d, c'_{y_i} = g^{s_i \cdot d} \cdot g^{y_i}, i \in [1, n]). \quad (9)$$

接着, 初始密文 C_0 经由地面段 CSP 被传输至 PS 处. PS 随机挑选 $\varphi \in \mathbb{Z}_p^*$ 混淆初始密文 C_0 . PS 计算 $g^\varepsilon = g^\varphi \cdot g^d$. 由上式可知 $\varepsilon = \varphi + d$. 根据上述步骤, PS 可以再次加密初始密文 C_0 , 得到最终密文 C .

$$C = (c_D = \mathcal{D}_L \cdot e(g, g)^{\beta \cdot \varepsilon}, c = g^\varepsilon, c_{y_i} = g^{s_i \cdot \varepsilon} \cdot g^{y_i}, i \in [1, n]). \quad (10)$$

最终密文 C 将被传输至 CSP 处存储.

(4) 加密索引生成 $IndexBuild(id, \vec{v}_L, pp, pk) \rightarrow I$. DO 输入层级标识 id 以及由多模态数据 $\mathcal{D}_L$ 提取出的特征向量 $\vec{v}_L$, 输出加密索引 I . 将 $\vec{v}_L$ 的第 i 位元素记作 $\vec{v}_L^{(i)}$, 由此可以构造如式 (11) 所示的索引.

$$I = (I_1, I_2) = (g^{\sum_{i=1}^m \vec{v}_L^{(i)}}, g^{\lambda \sum_{i=1}^m \vec{v}_L^{(i)}}). \quad (11)$$

最终, 索引 I 被发送至地面段的 CSP 处存储保管.

(5) 用户搜索 $Search(\mathcal{D}_q, Tok, I, sk) \rightarrow \hat{C}$. 该算法共分为两步, 包括 DU 侧查询陷门生成以及 CSP 侧数据搜索.

首先, DU 输入待查询的多模态数据 $\mathcal{D}_q$, 使用 5.1 小节介绍的特征提取方法得到查询特征向量 $\vec{v}_q$. DU 挑选一个随机元素 $t \in \mathbb{Z}_p^*$, 并利用持有的搜索令牌 Tok 和密钥 sk_{DU} 生成如式 (12) 所示的查询陷门 T .

$$\begin{aligned} T &= (td_1, td_2, td_3, td_4) \\ &= (g^{-pt \sum_{i=1}^m \vec{v}_q^{(i)}}, h^{pt^2}, h^{t^2 \sum_{i=1}^m \vec{v}_q^{(i)}}, \{h^{V_{att_i} \cdot t}\}_{att_i \in S_{DU}}), \end{aligned} \quad (12)$$

其中 att_i 为系统属性集 S 的第 i 个属性. 对于属性集为 S_{DU} 的用户 DU, td_4 可以表示为 $\{h^{V_{att_1} \cdot t}, h^{V_{att_2} \cdot t}, \dots, h^{V_{att_L} \cdot t}\}$.

随后, DU 将查询陷门 T 传输给 PS, 由 PS 向 CSP 进行查询请求. CSP 输入查询陷门 T 与加密索引 I , 根据系统设定的匹配算法进行数据匹配. 如果 DU 属性集 S_{DU} 满足机密层级 L 的访问策略, 同时待查询数据与数据库中已有数据一致, 则有以下式成立:

$$e(I_1 \cdot I_2, td_2) \cdot e\left(td_1, \prod_{att_i \in S_{DU}} td_{4,i}\right) = e(pk_{DU}, td_3). \quad (13)$$

待完成上述匹配算法后, CSP 最终得到结果密文 $\hat{C}$, 并将其传输给 PS.

(6) 数据解密 $Decrypt(\hat{C}, (pk, sk), SK) \rightarrow \hat{D}$. 为实现用户段 DU 的轻量级计算, PS 为 DU 计算解密参数. DU 将其属性密钥 SK 中的 $(SK_{\vec{x}}, SK_i)$ 上传至 PS 处, 由 PS 计算如式 (14) 所示的解密参数 par .

$$\begin{aligned} par &= \prod_{i=1}^n e(SK_i, c_{x_i}) \cdot e(SK_{\vec{x}}, c^{-1}) \\ &= e(g, g)^{\lambda \cdot \sum_{n=1}^n x_i \cdot y_i - \varepsilon(\lambda \xi + \beta)}. \end{aligned} \quad (14)$$

若 DU 满足第 L 层的访问策略, 由上文可知, $\vec{x} \cdot \vec{y} = 0$. 因此, 解密参数可化简为如下形式:

$$par = e(g, g)^{\lambda \cdot \sum_{n=1}^n x_i \cdot y_i - \varepsilon(\lambda \xi + \beta)} = e(g, g)^{-\varepsilon(\lambda \xi + \beta)}. \quad (15)$$

DU 在接收到解密参数 par 与结果密文 $\hat{C}$ 后, 进行轻量级数据解密:

$$\begin{aligned} &c_D \cdot par \cdot e(SK_0, c) \\ &= \hat{D} \cdot e(g, g)^{\beta \cdot \varepsilon} \cdot e(g, g)^{-\varepsilon(\lambda \xi + \beta)} \cdot e(g^{\lambda \cdot \xi}, g^\varepsilon) \\ &= \hat{D}. \end{aligned} \quad (16)$$

最终得到 DU 查询的多模态数据 $\hat{D}$.

6 方案分析

6.1 正确性分析

本节将对 SHMDS-SI 方案的正确性进行分析. 若用户搜索算法 *Search* 中的数据匹配机制以及数据解密算法 *Decrypt* 是正确的, 那么该方案是可行的.

当 CSP 输入查询陷门 T 以及索引 I 后, 若陷门对应的查询数据与索引对应的数据相匹配, 则有 $\sum_{i=1}^m \vec{v}_L^{(i)} = \sum_{i=1}^m \vec{v}_q^{(i)}$; 若数据用户 DU 的属性集 S_{DU} 满足机密层级 L 的属性策略, 则 $\lambda = \sum_{i \in S_{DU}} V_i$. 那么有如下匹配公式成立:

$$\begin{aligned}
 & e(I_1 \cdot I_2, td_2) \cdot e(td_1, \prod_{i \in S_{DU}} td_{4,i}) \\
 &= e(g^{\sum_{i=1}^m \vec{v}_L^{(i)}} \cdot g^{\lambda \sum_{i=1}^m \vec{v}_L^{(i)}}, h^{pt^2}) \cdot e(g^{-pt \sum_{i=1}^m \vec{v}_q^{(i)}}, \prod_{i \in S_{DU}} h^{V_i \cdot t}) \\
 &= e(g^{\sum_{i=1}^m \vec{v}_L^{(i)}}, h^{pt^2}) \cdot e(g^{\lambda \sum_{i=1}^m \vec{v}_L^{(i)}}, h^{pt^2}) \cdot e(g^{-pt \sum_{i=1}^m \vec{v}_q^{(i)}}, h^{\lambda t}) \\
 &= e(g^{\sum_{i=1}^m \vec{v}_L^{(i)}}, h^{pt^2}) \\
 &= e(g^p, h^{t^2 \sum_{i=1}^m \vec{v}_q^{(i)}}) \\
 &= e(pk_{DU}, td_3).
 \end{aligned} \tag{17}$$

DU 将属性密钥 SK 中的 $(SK_{\bar{x}}, SK_i)$ 发送给 PS, 由 PS 进行解密参数 par 的计算, 计算正确性验证如式 (18) 所示:

$$\begin{aligned}
 par &= \prod_{i=1}^n e(SK_i, c_{x_i}) \cdot e(SK_{\bar{x}}, c^{-1}) \\
 &= \prod_{i=1}^n e(g^{\lambda \cdot x_i}, g^{s_i \cdot \varepsilon + y_i}) \cdot e(g^{\lambda(\sum_{i=1}^n s_i \cdot x_i + \xi) + \beta}, g^{-\varepsilon}) \\
 &= e(g, g)^{\sum_{i=1}^n (\lambda x_i s_i \varepsilon + \lambda x_i y_i)} \cdot e(g, g)^{-\lambda \varepsilon \sum_{i=1}^n s_i x_i - \varepsilon(\lambda \xi + \beta)} \\
 &= e(g, g)^{\lambda \cdot \sum_{i=1}^n x_i \cdot y_i - \varepsilon(\lambda \xi + \beta)}.
 \end{aligned} \tag{18}$$

基于上述解密参数的正确性, DU 可以利用属性密钥 SK 中的 SK_0 进行轻量级运算解密得到多模态数据明文 $\hat{D}$.

6.2 隐私性分析

在本文讨论的卫星互联网系统中, 隐藏多模态数据明文的密文 C 以及隐藏特征向量信息的索引 I , 查询陷门 T 被保存在半可信机构 CSP 以及代理服务器 PSs 中. 半可信机构会积极地根据所拥有的数据推断隐私数据, 下文将对密文 C 以及索引 I , 查询陷门 T 的隐私性进行分析.

(1) 密文 C : 多模态数据密文 C 的构造方式为

$$C = (c_D = D_L \cdot e(g, g)^{\beta \cdot \varepsilon}, c = g^\varepsilon, c_{y_i} = g^{s_i \cdot \varepsilon} \cdot g^{y_i}, i \in [1, n]), \tag{19}$$

其中与数据明文相关的公式为 $D_L \cdot e(g, g)^{\beta \cdot \varepsilon}$. 对于代理服务器 PSs, 其所掌握的密文 $D_L \cdot e(g, g)^{\beta \cdot d}$ 中, d 为 DO 选取的随机数, 仅由 DO 掌握; 对于云服务提供商 CSP, 密文 $D_L \cdot e(g, g)^{\beta \cdot \varepsilon}$ 中的参数 ε 对 CSP 是保密的. 根据离散对数问题 (DLP), 半可信机构无法从密文中推断出隐私数据信息. 因此, 密文 C 具有隐私性.

(2) 索引 I 与查询陷门 T : 在索引 I 与查询陷门 T 的构造过程中, 与隐私特征向量相关的公式分别为 $(g^{\sum_{i=1}^m \vec{v}_L^{(i)}}, g^{\lambda \sum_{i=1}^m \vec{v}_L^{(i)}})$ 与 $(g^{-pt \sum_{i=1}^m \vec{v}_q^{(i)}}, h^{t^2 \sum_{i=1}^m \vec{v}_q^{(i)}})$. 首先, 将特征向量的各维度数据进行求和, 攻击者最多可以获得特征向量各维度数据的总和, 而无法得到特征向量的具体信息. 其次, 特征向量被置于指数位置, 根据离散对数问题 (DLP), 攻击者无法在多项式时间内恢复指数上的内容. 因此, 索引 I 与查询陷门 T 具有隐私性.

此外, 攻击者可以收集多个查询陷门并分析其关联性进行伪造. 下面对查询陷门 T 的不可链接性进行分析.

DU 在构造查询陷门 T 时, 会挑选随机元素 t 用于查询陷门 T 的生成过程, 如式 (12) 所示. 对于每个查询陷门 T , 其使用的随机元素 t 都是独立生成的. 这意味着, 同一用户 DU 生成的查询陷门 T 都是不同的. 因此, 查询陷门 T 具有不可链接性.

6.3 安全性分析

在选择明文攻击 (CPA) 背景下, SHMDS-SI 方案的密文 C 具备不可区分性.

定理2 若存在一个敌手 $\mathcal{A}$, 可以在概率多项式时间 (PPT) 内以不可忽略的优势 ϵ 破解 SHMDS-SI 方案的 CPA 安全模型, 那么可以构造一个模拟器 $\mathcal{B}$, 以 $\frac{\epsilon}{2}$ 的概率解决 DBDH 问题.

证明 挑战者 $\mathcal{Chal}$ 生成两个阶为大素数 p 的乘法循环群 G, G_T , 并挑选生成元 $g \in G$. 选择随机元素 $p, q, s \in \mathbb{Z}_p^*$ 以及 $T_R \in G_T$. 挑战者 $\mathcal{Chal}$ 随机选择 $b \in \{0, 1\}$, 若 $b = 0$, 我们设 $T_R = e(g, g)^{pqs}$; 否则, T_R 为群 G_T 的随机元素. 挑战者 $\mathcal{Chal}$ 将参数 (g, g^p, g^q, g^s, T_R) 交给模拟器 $\mathcal{B}$, 由模拟器 $\mathcal{B}$ 充当挑战者的角色进行 DBDH 问题的挑战.

(1) 初始化: 模拟器 $\mathcal{B}$ 运行如下所示的初始化函数 *Setup*.

模拟器 $\mathcal{B}$ 随机选择 $\alpha' \in \mathbb{Z}_p^*$, 并计算 $\alpha = \alpha' + pq$. 基于此, 有 $e(g, g)^{pq} \cdot e(g, g)^{\alpha'} = e(g, g)^\alpha$.

最后, 模拟器 $\mathcal{B}$ 输出公共参数 pp :

$$pp = \{G, G_T, p, e, g, g^s, e(g, g)^\alpha\}, \quad (20)$$

模拟器 $\mathcal{B}$ 将公共参数 pp 发送给敌手 $\mathcal{A}$.

(2) 查询阶段 1: 敌手 $\mathcal{A}$ 任意挑选消息 D 并将其提交给模拟器 $\mathcal{B}$. 模拟器 $\mathcal{B}$ 对消息 D 运行加密算法 *Encrypt*, 并输出密文 C^* , 将其发送给敌手 $\mathcal{A}$.

基于公共参数 pp , 模拟器 $\mathcal{B}$ 计算密文 C^* , 如下式所示:

$$C^* = D \cdot e(g, g)^{\alpha s} = D \cdot e(g, g)^{\alpha' s} \cdot e(g, g)^{pqs}. \quad (21)$$

(3) 挑战: 敌手 $\mathcal{A}$ 挑选两个等长的数据消息 D_0, D_1 , 要求其不能与查询阶段 1 中查询过的消息相同. 模拟器 $\mathcal{B}$ 选择随机数 $b \in \{0, 1\}$ 并计算如下密文 C_b :

$$C_b = D_b \cdot T_R \cdot e(g, g)^{\alpha' s}. \quad (22)$$

密文 C_b 被发送给敌手 $\mathcal{A}$.

(4) 查询阶段 2: 查询方式与查询阶段 1 相同, 但查询消息不能与 D_0, D_1 相同.

(5) 猜测: 敌手 $\mathcal{A}$ 基于查询结果与返回的密文 C_b 进行猜测, 输出 $b' \in \{0, 1\}$.

(i) $b' = b$: 模拟器 $\mathcal{B}$ 输出 0, 即 $T_R = e(g, g)^{pqs}$. 此时密文 C_b 有效, 敌手 $\mathcal{A}$ 以不可忽略的优势 ϵ 赢得游戏. 模拟器 $\mathcal{B}$ 在该情况下的解决概率满足 $\Pr[\mathcal{B}(g, g^p, g^q, g^s, T_R = e(g, g)^{pqs}) = 1] = \epsilon + \frac{1}{2}$.

(ii) $b' \neq b$: 模拟器 $\mathcal{B}$ 输出 1, 即 T_R 为随机数. 敌手 $\mathcal{A}$ 不具有赢得游戏的优势, 此时敌手 $\mathcal{A}$ 的获胜概率为 $\frac{1}{2}$. 模拟器 $\mathcal{B}$ 在该情况下的解决概率满足 $\Pr[\mathcal{B}(g, g^p, g^q, g^s, T_R \in G_T) = 1] = \frac{1}{2}$.

因此, 模拟器 $\mathcal{B}$ 解决 DBDH 问题的优势为

$$Adv = \left| \Pr[b' = b] - \frac{1}{2} \right| = \left| \frac{1}{2} \left(\frac{1}{2} + \epsilon + \frac{1}{2} \right) - \frac{1}{2} \right| = \frac{\epsilon}{2}. \quad (23)$$

7 性能分析

7.1 理论性能分析

为了展示 SHMDS-SI 方案相较于其他相近方案的性能优势, 本节对 SHMDS-SI 方案进行理论层面的功能、计算开销与通信开销分析, 并将其与近年所提出的方案进行对比, 包括 Zheng 等提出的 SFMS-CC^[12]、Yin 等提

表 2 功能特性对比.

Table 2 Comparison of functions.

Scheme	Multi-modal data feature extraction	ABSE	Policy hiding	Lightweight decryption for DUs
SFMS-CC ^[12]	×	✓	×	✓
DCP-ABSE ^[22]	×	✓	×	×
FE-ABSE-RV ^[25]	×	✓	✓	✓
CV-ABSE ^[26]	×	✓	×	×
EMK-ABSE ^[27]	×	✓	×	✓
ABSE-IIoT ^[28]	×	✓	✓	✓
SHMDS-SI	✓	✓	✓	✓

表 3 计算开销对比.

Table 3 Comparison of computational cost.

Scheme	Encryption of DO	Index generation	Trapdoor generation	Search	Decryption of DUs
SFMS-CC ^[12]	$4E + E_T$	$f \cdot E$	$4E$	$3E_T$	E_T
DCP-ABSE ^[22]	$2f \cdot E$	$f \cdot (E + E_T)$	$3E$	$(2f + 1)E_T$	$E + E_T$
FE-ABSE-RV ^[25]	$(2N + m + 1)E$ $+ E_T + mB$	$(f + 3) \cdot E$	$(f + 2)E + NB$	$4B$	$B + E + E_T$
CV-ABSE ^[26]	$(2f + M + 4)E$ $+(f + M)T_m + T_h + B$	$(2f + 2) \cdot E$	$(f + 3)E$ $+(f + 1)T_m + f \cdot T_h$	$f \cdot T_m + B$	$3(E + T_m)$
EMK-ABSE ^[27]	$(N + 3)E + B$	$(f + 3) \cdot E$	$3E$	$(f + 3)B$	B
ABSE-IIoT ^[28]	$E_T + N \cdot E$	$f \cdot E_T + N \cdot E$	$3E$	$(2 + N)E_T$	E_T
SHMDS-SI	$E + f \cdot B$	$2f \cdot E$	$(N + 3)E$	$(N + 2)B$	$E_T + T_d$

出的 DCP-ABSE^[22]、Chen 等提出的 FE-ABSE-RV^[25]、Niu 等提出的方案^[26]、Liu 等提出的 EMK-ABSE^[27]以及 Yin 等提出的方案^[28]. 为简便表述, 我们将文献^[26]中的方案简记为 CV-ABSE, 将文献^[28]中的方案简记为 ABSE-IIoT.

表 2 给出了 SHMDS-SI 方案与其余方案在功能特性方面的对比. 从表中可以看出, 所有方案均实现了基础的属性基可搜索加密功能. 然而, 仅 SHMDS-SI 方案具备多模态数据特征提取的能力, 实现了面向多模态数据的数据安全共享方案. SFMS-CC, DCP-ABSE, CV-ABSE 与 EMK-ABSE 方案不支持基于策略隐藏的属性基加密, 难以满足高隐私性保护需求. 此外, DCP-ABSE 与 CV-ABSE 方案缺乏终端轻量级解密能力, 对用户的计算资源提出了更高的要求. 相较而言, SHMDS-SI 方案不仅弥补了上述不足, 同时支持策略隐藏以及终端轻量级解密功能, 更创新性地集成了多模态数据特征提取能力. 因此, SHMDS-SI 方案在功能特性上相较其余方案具有更大优势.

在对比过程中所涉及的符号描述如下: E, E_T 分别代表群 G, G_T 上的模指数运算, B 代表一次双线性映射计算. f, m 分别代表数据集的大小与特征向量的维度. 定义 N 为系统属性集的大小, M 为满足访问策略的最小属性集大小. 在 CV-ABSE 方案中, T_m, T_h 分别代表乘法运算时间与哈希函数运算时间. 在 SHMDS-SI 方案中, T_d 代表一次除法运算的时间.

表 3 为各方案计算开销的对比, 主要包括 DO 侧加密、索引生成、查询陷门生成、搜索、DU 侧解密等过程. 首先, SHMDS-SI 方案在 DO 侧加密的开销为 $E + f \cdot B$, 即一次群 G 上的操作以及与文件集大小相关的双线性映射计算操作. 相较之下, FE-ABSE-RV 方案在 DO 侧的加密需要更多的群 G 与 G_T 上的操作; 而 CV-ABSE 方案需要更多开销实现乘法运算与哈希函数运算, 无法达到 DO 侧的轻量级计算. 对于索引生成开销, 各方案均为多次与文件集大小相关的群 G 上的运算, 并无明显差别. SHMDS-SI 方案在查询陷门生成的计算开销为 $(N + 3)E$, 这是因为本文将属性基令牌嵌入查询陷门中. 尽管如此, SHMDS-SI 方案依然比其余方案有更低的计算开销. 搜

表 4 存储开销对比.

Table 4 Comparison of storage cost.

Scheme	Key size	Index size	Trapdoor size	Ciphertext size
SFMS-CC ^[12]	$(N+2) G + \mathbb{Z}_p^* $	$f \cdot G $	$(f+3) G + (f+1) \mathbb{Z}_p^* $	$(f+1) G + (f+2) \mathbb{Z}_p^* $
DCP-ABSE ^[22]	$3 G + N \mathbb{Z}_p^* $	$f \cdot (G + G_T)$	$3 G $	$2f \cdot G $
FE-ABSE-RV ^[25]	$(2N+2) G + \mathbb{Z}_p^* $	$(f+3) \cdot G $	$4 G $	$(2m+1) G + G_T $
CV-ABSE ^[26]	$(N+3) G + \mathbb{Z}_p^* $	$(2f+2) \cdot G $	$(f+2) G + f \cdot \mathbb{Z}_p^* $	$(f+3M) G + G_T $
EMK-ABSE ^[27]	$(N+3) G + \mathbb{Z}_p^* $	$(f+3) \cdot G $	$4 G $	$(2N+5) G $
ABSE-IIoT ^[28]	$(2N+1) G $	$f \cdot G_T + N \cdot G $	$3 G $	$f G_T + (f+N) G $
SHMDS-SI	$(N+1) G $	$2f \cdot G $	$(N+3) G $	$ G + f \cdot G_T $

索过程一般由云服务提供商 CSP 实现, 因此 SHMDS-SI 方案的搜索计算开销尽管为多次较慢的双线性映射操作, 也并不会导致系统的堵塞. 最后, SHMDS-SI 方案在 DU 侧解密的计算开销为 $E_T + T_d$, 方案将双线性映射操作转移至代理服务器处, 剩余的除法运算操作相较其余方案包含的双线性映射操作开销更小, 提升了算法的效率.

表 4 为方案间存储开销对比, 包括密钥大小、索引大小、查询陷门大小与密文大小. 表中 $|G|$, $|G_T|$, $|\mathbb{Z}_p^*|$ 分别为群 $G, G_T, \mathbb{Z}_p^*$ 所占存储空间的大小. 在密钥存储开销方面, 由于表中方案均以属性基加密为基础, 生成密钥的方式相似, 密钥大小也较相似. 其次, SHMDS-SI 方案的索引大小为 $2f \cdot |G|$, 而索引在 DO 侧生成后被传输至 CSP 存储. 因此, SHMDS-SI 方案的索引存储开销可以忽略. 由于本文的陷门中嵌入了用户属性, 查询陷门大小与属性集大小相关. 相较于其他方案与文件集大小相关的陷门, 在云环境下文件集大小远大于属性集大小, 因此 SHMDS-SI 方案的查询陷门存储开销是最小的. 最后, SHMDS-SI 方案密文存储大小为 $|G| + f \cdot |G_T|$, 对比 SFMS-CC, FE-ABSE-RV, CV-ABSE 等方案开销更小, 是所有方案中存储开销最小的方案. 总之, SHMDS-SI 方案通过算法设计, 将较大的存储开销由地面段的云服务器承担, 实现了轻量级的存储.

7.2 仿真分析

7.2.1 方案性能对比

为了验证方案在真实多模态数据处理场景下的能力, 我们为每个模态都选取了真实且常用的数据集, 以此模拟真实多模态数据的输入. 针对文本、图像、音频数据, 我们分别使用 AG News, ImageNet, LibriSpeech 数据集进行实验. 此外, 还需要对数据集进行预处理使数据满足模型输入条件. 针对 AG News 数据集中的文本数据, 采用 WordPiece 进行分词处理, 并将序列最大长度设定为 128. 对于长度不足的序列进行零填充, 超长序列进行截断; 针对 ImageNet 数据集中的图像数据, 执行分辨率标准化操作, 通过双线性插值算法将所有输入图像的尺寸统一调整为 $224 \times 224 \times 3$ 像素, 以满足 ResNet-50 的输入维度要求; 针对 LibriSpeech 数据集中的音频数据, 首先通过重采样算法将所有音频数据的采样率统一转换为 16 kHz. 为了便于后续的统一特征映射, 我们将音频剪辑的时长标准化为固定窗口 (例如 3 s), 对短音频进行静音填充, 对长音频进行截断. 最后, 对音频波形执行幅度归一化, 消除录音设备差异带来的音量波动影响. 我们从三个数据集挑选等量的数据组成实验数据集, 作为实验的数据输入.

我们对 SHMDS-SI 方案在现实环境下的运行性能进行了仿真分析, 并将其与 SFMS-CC^[12], FE-ABSE-RV^[25], EMK-ABSE^[27] 的性能表现进行对比, 以此展现本方案的性能优势. 使用硬件配置为 2.50 GHz, 4 GB RAM, 操作系统为 Linux 的虚拟机进行仿真. 此外, 我们使用 Python 语言编写程序代码, 并借助 Charm 库实现双线性映射以及属性基加密的相关操作. 双线性映射的椭圆曲线参数为 “SS512”, 属性基加密的访问策略为简单的 “AND” 门.

在比较中, 我们设置了两个变量对 SHMDS-SI 方案的可搜索加密算法进行分析, 分别为特征向量维度与系统属性集大小. 图 6 展示了索引生成、陷门生成, 以及搜索算法在不同特征向量维度下的运行时间对比, 其中特

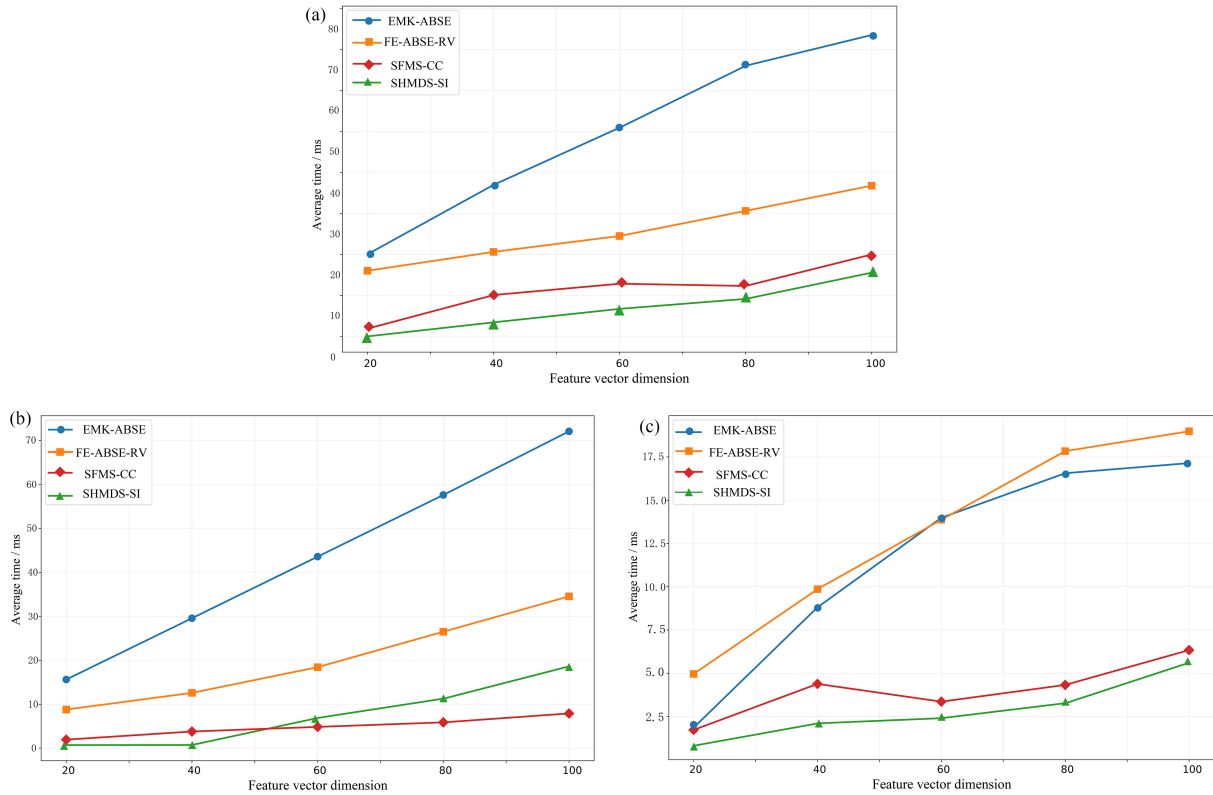


图 6 (网络版彩图) 不同特征向量维度下算法运行时间比较. (a) 索引生成; (b) 陷门生成; (c) 搜索.

Figure 6 (Color online) Comparison of algorithm running time under different feature vector dimensions. (a) Index generation; (b) trapdoor generation; (c) search.

征向量维度 $m \in [20, 100]$, 步长为 20. 图 7 给出了不同属性集大小下密钥生成、加密、解密、陷门生成算法的运行时间对比, 其中属性集大小 $n \in [10, 50]$, 步长为 10.

由图 6(a) 和 (b) 可知, 方案索引生成与陷门生成时间随特征向量维度增加呈线性增长的趋势. 其中, SHMDS-SI 方案在四个方案中索引生成耗时最少. 在维度 $m = 100$ 时, SHMDS-SI 方案仅需 17.4 ms 完成索引生成, 相较耗时最高的 EMK-ABSE 方案减少了近 70%; 在 $m = 40$ 时, SHMDS-SI 方案陷门生成耗时小于 SFMS-CC, 但之后其耗时较 SFMS-CC 增长较快. 由图 6(c) 可知, 方案搜索时间随特征向量维度增加而不断增加. SFMS-CC 与 SHMDS-SI 方案的搜索耗时相近, 较 FE-ABSE-RV 与 EMK-ABSE 方案更低, 搜索效率较高.

图 7 对 SHMDS-SI 方案的属性基加密开销进行了对比, SHMDS-SI 方案将属性嵌入陷门中实现访问控制, 因此我们还对不同属性集大小下的陷门生成进行了对比. 由图 7(a) 可知, 方案密钥生成耗时随系统属性集大小增加而线性增加, 由于 FE-ABSE-RV 与 SFMS-CC 方案为每一位用户生成独特的属性密钥, 因此耗时比 SHMDS-SI 方案大得多. 在加密过程中, SHMDS-SI 方案嵌入用户属性, 并借助 PS 二次加密提高安全性, 因此图 7(b) 中 SHMDS-SI 方案的加密耗时呈增长趋势. 由图 7(c) 可知, FE-ABSE-RV 与 HSES 方案的陷门生成时间与属性集大小相关. 在 $n = 50$ 时, SHMDS-SI 方案陷门生成耗时为 30 ms, FE-ABSE-RV 方案耗时为 36 ms, 开销降低约 17%. 由图 7(d) 可知, SHMDS-SI 方案解密时间在不同属性集大小下为常数, 原因是 SHMDS-SI 方案中解密开销被转移至 PSs, DU 侧解密只需轻量级计算. 随着属性集大小的增加, 其余方案的解密时间将远超 SHMDS-SI 方案.

由上述分析可知, 本文提出的 SHMDS-SI 方案在特征向量维度及属性集大小两种度量方式下相较其余方案均具有一定优势. 上述仿真分析证明了 SHMDS-SI 方案在现实环境下有较高的搜索效率和运行性能.

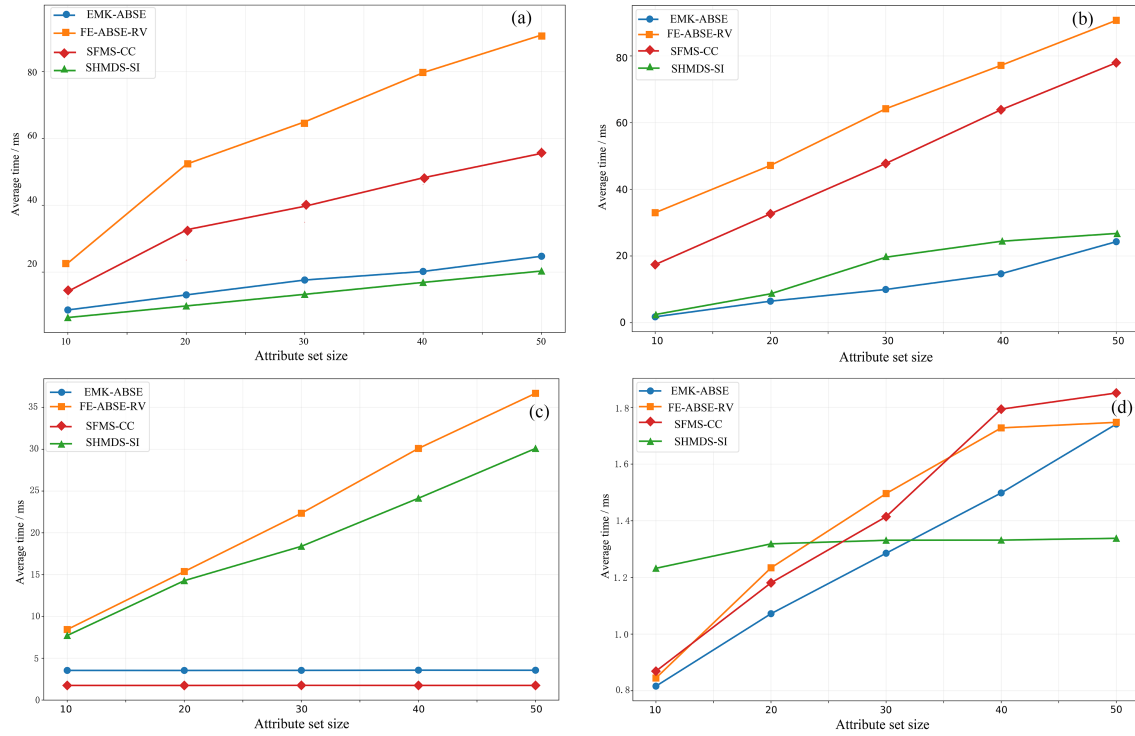


图 7 (网络版彩图) 不同属性集大小下算法运行时间比较. (a) 密钥生成; (b) 加密; (c) 解密; (d) 陷门生成.

Figure 7 (Color online) Comparison of algorithm running time under different attribute set sizes. (a) Key generation; (b) encryption; (c) decryption; (d) trapdoor generation.

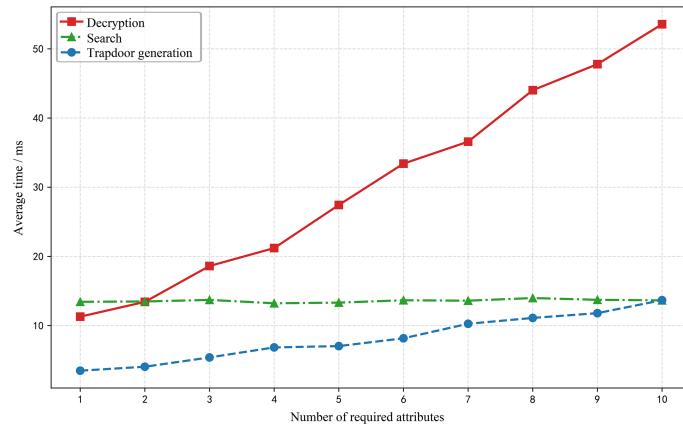


图 8 (网络版彩图) SHMDS-SI 方案 OR 策略下算法运行时间开销.

Figure 8 (Color online) Running time cost of algorithms under OR strategy of SHMDS-SI scheme.

7.2.2 OR 策略下的 SHMDS-SI 方案性能

为了进一步评估 SHMDS-SI 方案在处理复杂访问控制策略时的性能表现, 本节模拟了“OR”门限访问策略下, 算法运行时间随需满足属性数量变化的情况. 其中, 总属性数量为 10, 需满足的属性数量取值范围为 $[1, 10]$, 步长为 1, 记录陷门生成、搜索以及解密三个关键阶段的时间开销. 实验结果如图 8 所示.

对于搜索算法, 其运行时间几乎不随需满足属性数量的增加而波动, 维持在 13 ms 左右. 根据 SHMDS-SI 方案的搜索算法设计, 方案在匹配过程中采用了属性聚合机制, 尽管属性数量增加导致了群乘法运算次数的线性增长, 但由于群乘法的耗时远低于双线性对运算, 且方案将昂贵的双线性对运算次数固定为常数级, 因此总搜索

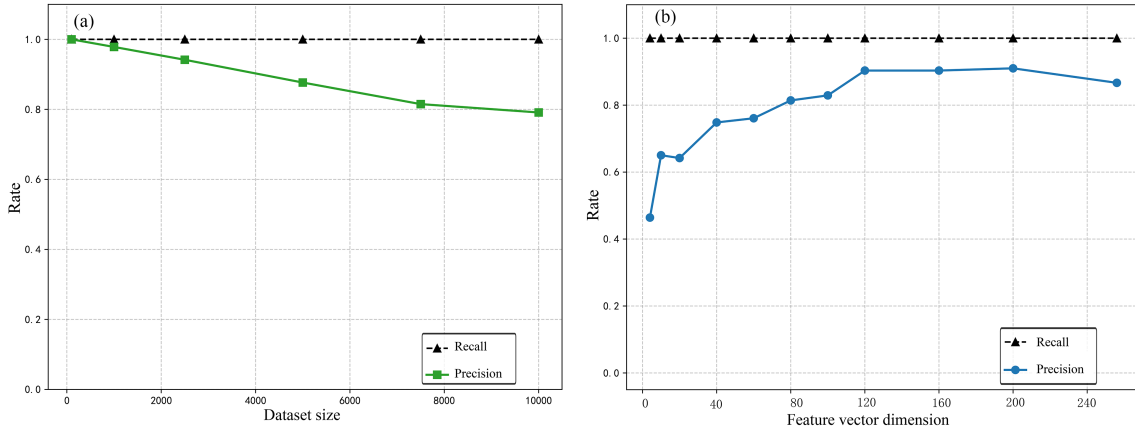


图 9 (网络版彩图) SHMDS-SI 方案的精确率与召回率. (a) 基于数据集大小变化; (b) 基于特征向量维度变化.

Figure 9 (Color online) Precision and recall of SHMDS-SI scheme. (a) Under dataset sizes; (b) under feature vector dimensions.

时间并未出现明显增加. 这表明本方案在大规模属性策略的检索场景下具有极高的效率和扩展性.

其次, 对于陷门生成算法, 其时间开销随着属性数量的增加呈现出平缓的线性增长趋势. 这是因为用户在生成陷门时, 需要针对每一个满足策略的属性执行模指数运算. 但整体耗时仍保持在较低的毫秒级水平, 证明了用户端计算的轻量化特性符合卫星互联网终端资源受限的要求.

最后, 解密算法运行时间随着需满足属性数量的增加呈现出显著的线性增长趋势, 且增长斜率较大. 这是因为在属性基加密机制中, 解密过程需要利用每一个满足策略的属性密钥进行昂贵的双线性对运算以恢复秘密值. 但是由于本方案将随策略复杂度线性增长的解密开销卸载至代理服务器 (PS), 有效避免用户设备因复杂访问策略而陷入计算瓶颈, 从而保障数据共享的实时性与可用性.

综上所述, SHMDS-SI 方案在 OR 策略下展现出了高效稳定的搜索能力和可控的终端计算开销, 能够良好地适应卫星互联网环境下灵活且复杂的细粒度访问控制需求.

7.2.3 SHMDS-SI 方案的精确率与召回率

检索准确性是衡量可搜索加密方案实用性的核心指标. 为了量化评估 SHMDS-SI 方案的检索性能, 我们将检索结果分为三类: 真阳性 (true positive, TP) 表示被正确检索到的目标数据; 假阳性 (false positive, FP) 表示被错误检索的非目标数据; 假阴性 (false negative, FN) 表示被遗漏的目标数据. 基于上述定义, 精确率 $Precision$ 与召回率 $Recall$ 的计算公式如下.

$$Precision = TP / (TP + FN), \quad (24)$$

$$Recall = TP / (TP + FP). \quad (25)$$

本节考虑数据集大小 f 与特征向量维度 m 两个关键变量对 SHMDS-SI 方案检索精确率和召回率的影响. 实验结果如图 9 所示. 在两种变量变化时, 方案的召回率始终稳定保持在 1.0. 由于陷门生成与索引构建均基于相同的特征提取算法, 对于任意真实匹配的数据项, 其特征向量和必然满足 $\sum \vec{v}_L = \sum \vec{v}_q$, 从而确保了 CSP 在执行搜索时不会遗漏任何符合条件的目标数据 (即不存在假阴性 FN).

图 9(a) 和 (b) 分别展示了数据集大小和特征向量维度对精确率的影响. 在图 9(a) 中, 实验设定特征维度 m 为定值, 数据集大小 f 从 100 增加至 10000. 结果显示, 随着数据规模的扩大, 精确率呈现出缓慢下降的趋势 (从接近 1.0 降至约 0.78). 这是因为 SHMDS-SI 方案采用特征向量求和作为匹配依据, 随着数据库中样本数量的增加, 不同特征向量产生相同和值, 即发生“碰撞”的概率会有所上升, 导致假阳性结果的出现. 尽管如此, 在大规模数据下精确率仍维持在可接受范围内. 在图 9(b) 中, 实验设定数据集大小 f 为定值, 特征维度 m 从 10 增加至 240. 此时精确率与特征维度呈显著的正相关关系. 在低维空间 (如 $m < 40$) 下, 由于特征表达的稀疏性, 向量

求和极易发生碰撞,导致精确率较低.然而,随着维度的增加,特征空间的表达能力显著增强,碰撞概率呈指数级下降.当特征向量维度超过 120 时,精确率稳定在 0.9 以上.

综上所述,SHMDS-SI 方案通过合理的参数设置(例如选择 $m \geq 128$),能够在保证 100% 召回率的前提下,实现高精度的多模态数据检索,满足卫星互联网对数据查询准确性的要求.

7.3 系统部署分析

7.3.1 通信开销分析

在卫星互联网中,尽管低轨卫星星座显著提升了通信带宽,但相较于地面光纤网络,星地链路依然昂贵且受限于复杂的通信环境.因此,通信开销对评估方案在实际工程中的可行性具有重要作用.本节结合现代宽带卫星通信场景,对 SHMDS-SI 方案的实际通信开销进行定量分析.

我们选取典型的现代宽带卫星上行链路作为通信场景,有效上行传输速率 $R = 20$ Mbps. 设定方案群元素大小 $|G| = 512$ bits, 属性集大小 $N = 50$, 数据集大小 $f = 10000$. 在评估中,我们忽略传播时延与排队时延的差异,对比各方案间发送时延的大小,其计算公式如下:

$$T_{trans} = \frac{L}{R}, \quad (26)$$

其中 L 为通信数据量. 由于有效上行传输速率一致,我们对各方案不同阶段的通信数据量进行对比. 搜索阶段的数据开销主要集中在用户段 DU 向 CSP 发送的查询陷门. 从表 4 以及上文存储开销分析可知,SHMDS-SI 方案的查询陷门大小为 $(N + 3)|G|$, 在所有方案中最小. 经过计算, SFMS-CC 方案的查询陷门数据量约为 625 kB, 而 SHMDS-SI 方案仅有 3.3 kB. 在相同带宽下, SHMDS-SI 方案的发送时延极低, 仅约 1.32 ms, 极大节省了上行链路的资源. 在数据传输阶段中, 通信开销主要由密文以及索引大小决定. SHMDS-SI 方案的密文大小为 $|G| + f \cdot |G_T|$, 对应的传输数据量大小约为 625 kB, 仅需 25 ms 即可完成传输; 索引大小为 $2f \cdot |G|$, 对应的传输数据量为 1250 kB, 发送延迟为 5 ms. 尽管现代宽带上行链路带宽有限, SHMDS-SI 方案的数据量大小仍在其可接受范围内, 且发送延迟维持在毫秒级, 保证了星地链路数据传输的可行性.

7.3.2 方案时延分析

为了更全面地评估 SHMDS-SI 方案的传输性能, 本节建立了一个端到端的时延计算模型. 通过考虑计算开销、传输带宽与往返时延 RTT, 计算用户从发起查询到最终得到明文的总时延. 总时延 T_{total} 计算方式为 $T_{total} = T_{prop} + T_{trans} + T_{comp}$. 其中 T_{prop} 为传播与排队时延, 主要由链路的物理距离以及网络排队决定, 本节中设置为一次往返; T_{trans} 为上文讨论的传输时延, 包括上行时延与下行时延; T_{comp} 为计算时延, 即陷门生成、搜索、解密等算法的执行时间.

根据 T_{total} 的计算方式以及理论性能分析中的数据, 本节分别计算了不同往返时延 RTT 和不同带宽下 SHMDS-SI 方案的运行总时延, 结果如图 10 所示.

图 10(a) 为不同 RTT 下 SHMDS-SI 方案的总时延变化, 计算时带宽固定为 20 Mbps. 由于往返时间增加, 系统运行总时延必然会增长, 因此总时延与 RTT 呈正相关. 然而, 尽管在 $RTT = 800$ 的通信环境下, 总时延也能控制在 1.3 s 左右, 除去物理传播的必要时间, 方案的计算与传输开销仅 0.5 s 左右, 确保了长通信距离下方案的可行性. 图 10(b) 展现了不同带宽下方案的总时延变化, 其中 RTT 固定为 10 ms. 结果表明, 随着带宽的增加, 即通信能力的增强, 方案的总时延可以达到 0.1 s. 在高带宽环境下, 方案总时延趋于平稳, 这说明 SHMDS-SI 方案对高带宽的依赖性不高, 在 40 Mbps 的常规商用带宽下即可实现性能饱和, 极大降低了部署成本. 即使在较差的通信环境下, 方案也可以实现较快的数据访问响应. 综上所述, 本节通过计算并分析不同 RTT 与传输带宽下的总时延大小, 证实了 SHMDS-SI 方案的部署可行性.

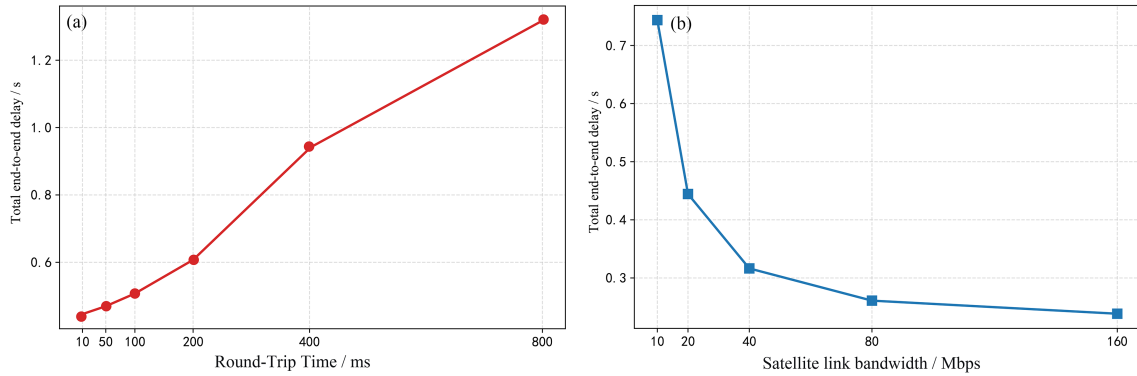


图 10 (网络版彩图) SHMDS-SI 方案端到端总时延. (a) 不同 RTT 下; (b) 不同带宽下.

Figure 10 (Color online) Total end-to-end delay of the SHMDS-SI scheme. (a) Under different RTTs; (b) under different bandwidths.

8 总结

针对多模态数据特征提取、细粒度访问控制以及云边端协同计算难题, 本文在卫星互联网环境下构建了一种多模态数据层次可搜索加密方案. 方案通过特异性的特征提取方式, 实现异构多模态数据的统一化处理; 基于可搜索加密与属性基加密的结合, 构建安全的属性基可搜索加密机制, 实现高效搜索与细粒度访问控制的结合; 通过设计云边端协同计算框架, 引入代理服务器降低用户段终端设备的开销. 此外, 我们已经对方案的隐私性以及安全性进行了严谨的证明, 分析表明方案满足 CPA 安全, 同时方案中的密文具备良好的隐私性.

在未来的研究中, 我们将对算法的复杂度进行进一步优化, 提升方案在大规模数据处理场景下的高效性. 此外, 我们将对方案在更加复杂的卫星互联网环境下的部署进行探索, 如加入空中段的天地一体卫星互联网, 进一步提高方案的适应性与可行性.

参考文献

- 1 Coombs M L, Cameron C E, Dietterich H R, et al. From field station to forecast: managing data at the Alaska Volcano Observatory. *Bull Volcanol*, 2024, 86: 79
- 2 Zhao H, Cen S, Zhu Y F. The space above the sky: uniting global-scale ground station as a service for efficient orbital data processing. In: *Proceedings of IEEE 32nd International Conference on Network Protocols (ICNP)*, 2025
- 3 Cao Q. An investigation on the convergence of satellite Internet and 5G mobile communication. In: *Proceedings of International Conference on Green Communication, Network, and Internet of Things*, 2023. 80
- 4 Zhao F, Zhang C C, Geng B C. Deep multimodal data fusion. *ACM Comput Surveys*, 2024, 56: 1–36
- 5 Bayoudh K. A survey of multimodal hybrid deep learning for computer vision: architectures, applications, trends, and challenges. *Inf Fusion*, 2024, 105: 102217
- 6 Dhaygude A D, Varma R A, Yerpude P, et al. Deep learning approaches for feature extraction in big data analytics. In: *Proceedings of 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 2023. 964–969
- 7 Hu J, Shen L, Albanie S, et al. Squeeze-and-excitation networks. *IEEE Trans Pattern Anal Mach Intell*, 2020, 42: 2011–2023
- 8 Liu X Y, Qiu H J, Li M Q, et al. Application of multimodal fusion deep learning model in disease recognition. In: *Proceedings of 2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*, 2024. 1246–1250
- 9 Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: *Proceedings of 2000 IEEE Symposium on Security and Privacy*, 2000. 44–55
- 10 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: *Proceedings of 2007 IEEE Symposium on Security and Privacy (SP'07)*, 2007. 321–334
- 11 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 2006. 89–98
- 12 Zheng K, Zhou Z, Liu J, et al. Secure fine-grained multi-keyword ciphertext search supporting cloud-edge-end collaboration in IoT. *Chin J Elect*, 2025, 34: 266–281

- 13 Tang L Z, Zhong C S, Sun Z X. BMF-CP-ABE: blockchain-based multi-keyword fuzzy searchable attribute-based encryption scheme. In: Proceedings of 2025 37th Chinese Control and Decision Conference (CCDC), 2025. 3322–3329
- 14 Bala A, Rashid R Z J A, Ismail I, et al. Artificial intelligence and edge computing for machine maintenance-review. *Artif Intell Rev*, 2024, 57: 119
- 15 Miao Y B, Ma J F, Zhang J W, et al. Efficient verifiable multi-keyword search over encrypted data. *J Xidian Univer*, 2017, 44: 18
- 16 Gu K, Zhang W, Li X, et al. Self-verifiable attribute-based keyword search scheme for distributed data storage in fog computing with fast decryption. *IEEE Trans Netw Serv Manage*, 2022, 19: 271–288
- 17 Shi J, Yu Y, Yu Q, et al. Toward data security in 6G networks: a public-key searchable encryption approach. *IEEE Netw*, 2022, 36: 166–173
- 18 Xu C, Wang N, Zhu L, et al. Achieving searchable and privacy-preserving data sharing for cloud-assisted e-healthcare system. *IEEE Internet Things J*, 2019, 6: 8345–8356
- 19 Zhou F, Zhang Z, Hou R. Privacy-preserving image retrieval with multi-modal query. *Comput J*, 2023, 67: 1979–1992
- 20 Xu Y, Zhang M Y, Li C X, et al. MMQ: multimodal mixture-of-quantization tokenization for semantic ID generation and user behavioral adaptation. 2025. ArXiv:2508.15281
- 21 Zhang T, Shi M. Multi-modal neuroimaging feature fusion for diagnosis of Alzheimer's disease. *J Neurosci Methods*, 2020, 341: 108795
- 22 Yin H, Zhao Y, Zhang L, et al. Attribute-based searchable encryption with decentralized key management for healthcare data sharing. *J Syst Architecture*, 2024, 148: 103081
- 23 Mamta, Gupta B B. An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud. *Concurrency Computation*, 2020, 32: e5291
- 24 Shen Z S, Jin J, Tan C, et al. A survey of next-generation computing technologies in space-air-ground integrated networks. *ACM Comput Surveys*, 2023, 56: 1–40
- 25 Chen L, Xu S, Zhang H, et al. Fair-and-exculpable-attribute-based searchable encryption with revocation and verifiable outsourced decryption using smart contract. *IEEE Internet Things J*, 2025, 12: 4302–4317
- 26 Niu S F, Chen L X, Liu W K. Attribute-based keyword search encryption scheme with verifiable ciphertext via blockchains. In: Proceedings of 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2020. 849–853
- 27 Liu J, Li Y, Sun R, et al. EMK-ABSE: efficient multikeyword attribute-based searchable encryption scheme through cloud-edge coordination. *IEEE Internet Things J*, 2022, 9: 18650–18662
- 28 Yin H, Zhang W, Deng H, et al. An attribute-based searchable encryption scheme for cloud-assisted IIoT. *IEEE Internet Things J*, 2023, 10: 11014–11023

Secure hierarchical multi-modal data sharing scheme in satellite Internet

Kaifa ZHENG¹, Jiayi LIU², Gaopan HOU^{3*}, Liquan YANG⁴, Yinbin MIAO³ & Zhiquan LIU^{2*}

1. School of Information Engineering, Wuhan University of Technology, Wuhan 430070, China

2. College of Cyber Security, Jinan University, Guangzhou 511443, China

3. School of Cyber Engineering, Xidian University, Xi'an 710126, China

4. School of Cyber Science and Technology, Beihang University, Beijing 100191, China

* Corresponding author. E-mail: hougaopan@xidian.edu.cn, zqliu@vip.qq.com

Abstract With the development of satellite Internet, the volume of sensitive multi-modal data is constantly increasing, and its secure storage and access are facing great challenges. The existing data sharing schemes cannot balance search efficiency and privacy access control during the search process. To address the above contradictions, we propose a secure hierarchical multi-modal data sharing scheme in satellite Internet (SHMDS-SI), which ingeniously combines hierarchical access control with searchable encryption, achieving the secure sharing of multi-modal data in satellite Internet. Firstly, the scheme selects specific feature extraction methods to extract features from heterogeneous multi-modal data, and output feature vectors of unified dimensions, improving the efficiency of data processing. Secondly, the scheme designs policy-hidden attribute-based encryption and searchable encryption algorithms, embedding user attributes into data ciphertexts and trapdoors to achieve hierarchical fine-grained access control for encryption and search processes. Finally, the system, through the cloud-edge-end collaborative computation protocol, designates proxy servers to assist users in decryption, effectively reducing the high computing overhead of terminal devices. This paper provides a rigorous proof of the security of the scheme. Meanwhile, theoretical and simulation analyses show that this scheme has a higher search efficiency compared with the existing schemes.

Keywords satellite Internet, searchable encryption, multi-modal data security, attribute-based encryption, cloud-edge-end collaborative computation