并行属性基加密技术下物联网隐私数据安全共享算法

赵治斌[1] 冯 黎[1]
ZHAO Zhibin FENG Li

摘 要 物联网产生的数据来自众多不同的设备和数据源，当撤销某个属性时，需要给未受影响的数据重新生成新的密钥并进行分发和实时更新，而现有方法无法同时将不同属性组合的密钥生成任务分配到多个计算节点上，导致共享过程耗时耗力，且易引发操作失误，导致共享失败。为此，文章提出一种并行属性基加密技术下物联网隐私数据安全共享算法。先构建包含数据拥有者、用户、物联网云服务和授权机构的物联网隐私数据安全共享系统。在此系统架构下，引入由授权机构执行的并行属性基加密方法，数据拥有者借此对明文和公钥加密，用户依据自身属性集合与访问策略解密。通过并行处理将不同属性组合的密钥生成任务分配到多个计算节点上，提高加密和解密操作效率，解决属性多导致加密时间成本增加的问题。基于属性基加密技术进一步设计隐私数据共享协议机制，基于角色评估框架全面评估计算服务提供者、数据持有者和数据请求者的信誉。系统根据评估结果决定是否进行安全访问控制，确保物联网隐私数据共享的安全性与可用性，实现细粒度访问控制。实验结果表明，所提算法在保证物联网数据隐私的同时，降低了复杂性，有力保障了物联网数据的安全共享。

关键词 并行属性基加密；隐私数据；物联网；数据安全；数据共享

doi：10.3969/j.issn.1672-9528.2025.04.037

0 引言

随着物联网技术的快速发展，众多设备联网产生大量数据，其中包含个人身份、位置、健康状况和行为习惯等用户敏感信息。隐私数据在共享时若泄露或被不当使用，会给用户隐私、安全乃至社会稳定带来不可估量的损害[1]。虽然已有一些数据隐私保护算法和技术，但物联网设备资源受限、网络连接多样、数据海量且实时等特殊性质，使传统方法无法直接用于物联网环境。所以，深入研究物联网隐私数据安全共享算法、探索创新解决方案，是学术界研究热点。

目前，众多学者深入研究隐私数据安全共享算法。例如，文献 [2] 提出基于区块链的物联网数据安全共享机制，该机制利用区块链不可篡改和去中心化的特点，将设备访问控制规则和通信管理信息记录在区块链各区块上，防止设备未经授权访问和通信资源滥用。但该机制在调节设备访问权限时，需加密验证设备属性信息。设备众多且属性复杂，加密验证操作繁琐，可能产生延迟，错过数据传输最佳时机，使数据传输受干扰，误码率增加。文献 [3] 利用区块链构建“主从链”结构的跨域隐私数据共享模型，先构建主从链基础框架以规划整体架构，再用智能合约技术开发跨域访问控制机制，进而设计跨域安全共享策略保护隐私数据。针对海量属性，智能合约需逐个检查属性是否符合访问条件，验证过程涉及多次区块链查询和复杂逻辑判断，导致数据共享时间延长。

针对现有方法存在的不足，本文设计了一种适用于物联网隐私数据安全共享的并行属性基加密算法。

1 物联网隐私数据安全共享算法设计

1.1 构建物联网隐私数据安全共享系统模型

物联网设备的海量性和属性多样性导致了属性管理的极大复杂性，在面对这些数量庞大且属性各异的设备时，传统的安全共享算法采取了逐一进行加密和解密的处理方式，这不仅消耗了大量时间，还严重影响了系统的响应速度，导致隐私数据在传输过程中的误码率大幅上升，严重威胁到数据的安全性和完整性。为解决此弊端，本文提出采用并行属性基加密技术构建属性基加密系统模型。通过该加密技术，数据拥有者可以灵活地定义访问策略，在保护数据隐私的同时，实现物联网数据更精细的访问权限管理。

本文设计的属性加密系统包含数据拥有者、用户、物联网云服务及授权机构 4 大组成部分。该系统的架构如图 1 所示。

1. 兰州职业技术学院信息工程学院 甘肃兰州 730070

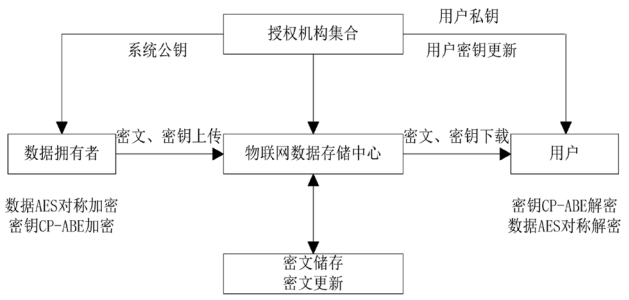

图 1 属性基加密技术的系统模型

数据拥有者是物联网数据共享行为的发起者和数据源提供者。用户需从授权机构获取私钥，只有属性符合访问控制要求时才能解密数据，确保访问权限管理。物联网云服务作为数据存储和访问中心，负责密文数据的存储、传输及属性变更时及时更新相应的密文数据，保障数据完整性和可用性。授权机构负责系统公共设置、密钥生成与分发，并在属性撤销时及时更新密钥，维护系统安全与稳定。

1.2 并行属性基加密方法的设计与实现

在物联网环境中，为实现隐私数据的细粒度访问控制，通常结合对称加密和属性加密技术，即对称加密保护数据块，属性加密保护对称密钥。然而，随着属性数量的增加，加密时间成本呈线性增长，尤其在物联网设备众多且属性繁杂的场景下，这种增长显著影响系统性能。此外，属性撤销时，传统方法需要为未受影响用户重新生成和分发密钥，并更新相关密文文件，这在大规模数据共享场景下带来巨大的时间和计算负担。为解决这些问题，本文提出了一种并行属性基加密方案，利用并行处理技术将密钥生成任务分配到多个计算节点，优化加密和解密性能，降低时间成本。通过分解加密和解密任务，并充分利用多核处理器或分布式计算资源，显著提升效率，特别是在处理大规模物联网数据时表现突出，有效解决了属性数量多和属性撤销带来的时间开销问题，全面提升了系统性能和用户体验。

并行属性基加密方案由授权机构执行，执行所需的信息包括全面的属性集合 s 和安全参数 ∂，其中，$S=\{S_1,S_2,\cdots,S_m\}$，S_m 代表第 m 个属性。并选定一个双线性对 b_h，利用该对产生两个生成元，分别进行标识为 j、l，b_h 的具体表示为：

$$b_h=\left(h_1,h_2,h_A,z,c\right) \tag{1}$$

式中：z、c 代表线性对；h_1、h_2、h_A 代表线性阈值。

选择一个随机参数 α，计算密钥的参数 d、f_i，以便同时生成多个密钥。d、f_i 用公式表示为：

$$\begin{aligned} d&=j^{\alpha}\\ f_i&=l^{\alpha} \end{aligned} \tag{2}$$

使用 d、f_i 生成主密钥与公钥，其表达公式为：

$$\begin{aligned} G_k&=\left\{b_h,l,d,f_i,h\left(j,l\right)\right\}\\ V_k&=\left\{\alpha,j\right\} \end{aligned} \tag{3}$$

式中：G_k 代表公钥；$h(j,l)$ 代表 j、l 的线性函数；V_k 代表主密钥。

将输入设定为属性集合 β、G_k、V_k，选取一个随机参数 χ，然后依据公式计算密钥 Y 的参数 c、c'：

$$\begin{aligned} c&=\sum_{i=1}^{m}\alpha^{ix_i}+m\\ c'&=\sum_{i=1}^{m}\alpha^{ix_i+1}+m\alpha \end{aligned} \tag{4}$$

式中：$\boldsymbol{x}_i$ 代表第 i 个随机向量，利用 c、c' 对密钥 Y 进行计算。

其次，数据所有者执行此方案，能够并行地对多个明文进行加密。对于明文 Z，数据所有者选择相应的访问规则、随机数值和随机向量 $\boldsymbol{u}_i$，并并行计算密文 E 中的参数 δ_1、δ_2、δ_3，结合该随机数值与参数 δ_1、δ_2、δ_3，即可还原出明文 Z。

用户运行该方案，输入 G_k、Y 以及明文 Z，用公式表示为：

$$\boldsymbol{u}_i\times\boldsymbol{x}_i\neq\boldsymbol{m} \tag{5}$$

证明用户的属性未达到 w 的要求，仅当用户的属性符合 w 的条件时，解密过程才能进行。并行解密时，需利用随机向量 $\boldsymbol{u}_i$ 和 $\boldsymbol{x}_i$ 来计算明文 Z 的参数，进而获取明文 Z。

并行属性基加密方案通过合理地将加密和解密任务进行分解，并充分利用多核处理器或分布式计算资源，能够显著提升加密和解密的效率。

1.3 隐私数据的共享与访问

通过对数据进行加密处理，可以确保数据在传输和存储过程中的安全性。然而，仅仅依靠加密技术并不足以完全保障数据的安全，因为数据的访问和使用同样需要得到有效的控制。对数据进行共享与用户信誉的评估，可以进一步确保只有符合特定条件（如信誉良好、权限合规等）的用户才能访问和使用数据，从而增强数据共享的安全性。通过评估用户的信誉和权限，并根据评估结果进行用户信誉的判定，以此作为数据是否安全访问控制的依据，进而实现数据的安全访问控制[4-5]。此过程涉及 3 个核心实体：监管中心、云存储器和授权机构。

隐私数据的共享协议设计如下：

用户提交注册信息后，监管中心依据这些信息授予权限。注册信息可表示为：

$$T=\{G_k,Y,p_i,R_k\} \tag{6}$$

式中：R_k 代表用户的属性私钥；p_i 代表数字证书。

数据所有者将元数据保存在云存储器中，同时将物联网中的隐私数据委托给授权机构进行保管。物联网隐私信息的使用权限被信息相关人控制，可以把信息共享给其他使用者[6-8]。同时，只有在数据关联者授权后，其他使用者方可取得存取授权或解密的数据。

其次，角色信誉的评价涵盖计算服务提供者、数据持有者及数据请求者的信誉评估。这一评价基于角色评估框架，针对交易活动进行[9-10]。该框架的核心在于依据共享状况进行评估，若共享未达成，则遵循以下具体评估标准：

在不同共享状态下，角色和记录行为有所不同：初始状态（initial）时，不作为角色和诚信角色均为空，且不记录共享失败或成功；确认计算状态（confirmedByCal）时，不作为角色为计算服务方，诚信角色为空，仅记录共享失败；获取数据状态（getData）时，不作为角色为数据所有者，诚信角色为计算服务方，仅记录共享失败；获取结果状态（getRes）时，不作为角色和诚信角色均为计算服务方，仅记录共享失败；完成状态（finish）时，不作为角色和诚信角色均为等待仲裁，仅记录共享失败。

最终进行用户的信誉评估，进而利用该公式进行数据是否安全访问控制的判断：

$$\eta=\begin{cases}\varpi\times a_\sigma\times\left(\dfrac{R_1}{\sum_{i=1}^{n}R_i}+\dfrac{K_1}{\sum_{i=1}^{n}K_i}\right), a_\sigma\neq 0\\ 0, a_\sigma=0\end{cases} \tag{7}$$

式中：η 为各角色信誉评分的总和；R_1 为角色成功共享的次数；R_i 为角色共享失败的次数；ϖ 为一个固定常数；n 为角色总的共享行为次数；K_1 为角色申诉成功的次数；K_i 为角色申诉失败的次数；a_σ 则反映了角色在申诉与共享活动中未参与的情况。

本文设计的这一算法将通过定义访问策略，将数据加密后存储在物联网设备或云端，只有满足特定属性条件的用户才能解密和访问数据。

2 实验测试与分析

2.1 实验准备

为验证本文所设计的属性基加密技术下物联网隐私数据安全共享算法的可行性，本次测试拟在确保密文数据隐私性的前提下，实现对密文数据的细粒度访问控制。基于 Matlab 软件搭建了一个仿真测试平台，具体参数如表 1 所示。

表 1 实验参数

参数	数值
操作系统	Linux ubuntu 14.04
CPU	Genuine Intel(R) T2080 @1.73 GHz
内存	32 GB
开发工具	属性基加密算法库 Hyperledger
物联网通信协议	MQTT、CoAP
智能合约	Go 语言

基于该测试平台，导入一个来自某市智能电网的物联网隐私数据集，并使用本文所提出的算法与文献 [2] 提出的跨域安全共享模型、文献 [3] 提出的结合区块链的物联网数据安全共享机制对该数据集进行安全共享测试。具体步骤如下：

（1）在物联网隐私数据集中的选定数据进行预处理，包括格式转换，数据清洗等。

（2）分别构建属性基加密方案与传统数据加密方案，在服务器上部署相应的算法库，并配置两种算法的访问控制策略。

（3）将隐私数据上传至服务器，服务器根据两种不同的访问控制策略对数据进行加密处理。用户根据自身属性向服务器请求数据访问权限，服务器根据访问策略判断用户是否有权访问数据。

（4）引入比特出错概率（BER）、共享时间衡量指标，比较三种算法在物联网环境下的数据共享效果。

2.2 实验结果与分析

基于上述实验准备内容，在物联网数据量不同的条件下，针对本文算法与传统算法开展了误码率（BER）测试，并得到了对比结果，如图 2 所示。

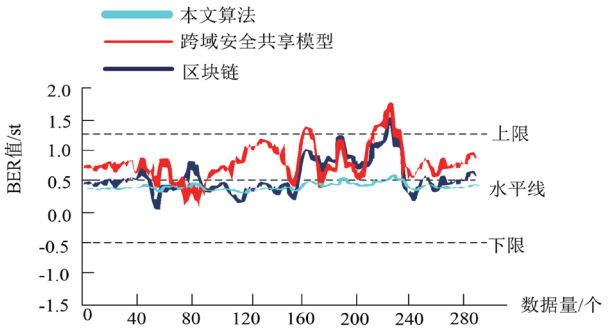

图 2 不同算法的 BER 测试结果

从图 2 中可以看出，与其他两种算法相比，本文安全共享算法的 BER 值更低。其他算法 BER 值超可接受上限，本文算法 BER 值稳定在较低且合理范围波动，最高仅约 0.6。这表明采用属性基加密技术的算法保密性能更优，能更有效保障物联网私密信息安全。本文算法优势在于引入并行属性基加密方法，该技术有细粒度访问控制能力，可依据用户属性集合和访问策略精确划分权限。这种加密方式提升了数据安全性，保证只有符合特定条件的用户能访问敏感数据，有效避免非法访问和数据泄露，从而使误码率较低。

较短的数据共享时间意味着算法在处理数据方面更加高效，能够更快地满足用户的需求。图 3 给出了本文算法、跨域安全共享模型和区块链方法在数据共享时间需求上的对比

测试结果。

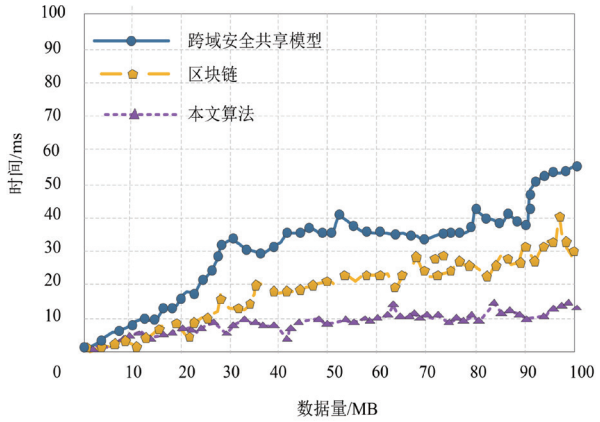

图 3 共享时间测试结果

根据图 3 的共享时间测试结果，可以分析得出：相较于跨域安全共享模型和区块链方法，本文提出的算法在数据共享时间上表现出更明显的优势，具有更高的处理效率和更快的响应速度，能够更迅速地满足用户对数据访问的需求。此优势得益于本文算法引入的并行属性基加密技术。数据共享时，加密和解密操作最耗时，本文算法采用并行处理技术可同时处理多个任务，大幅缩短共享时间，即便大数据量的加密解密需求也能迅速完成，有效提高了数据共享效率。

3 结语

本研究基于属性基加密技术的核心优势，设计了一种物联网数据安全共享算法，该算法不仅确保了数据的严格隐私保护，还实现了精细的访问控制和高效的数据共享。通过引入并行处理技术，显著提升了加密和解密操作的效率。同时，结合隐私数据共享协议机制和角色评估框架，系统能够智能地根据用户信誉和访问策略作出安全决策，进一步增强了物联网数据共享的安全性和可用性。然而，随着物联网的蓬勃发展和数据量的激增，对数据隐私保护与共享的技术要求也日益严格。未来，仍需不断探索和优化数据隐私保护技术，包括加密算法的升级、数据脱敏技术的创新以及访问控制策略的精细化设计。此外，研究数据合理共享的新模式，如利用匿名化技术和安全多方计算等方法，也是推动物联网数据安全共享技术发展的重要方向。

参考文献：

[1] 张克君，王文彬，徐少飞，等．面向云存储且支持重加密的多关键词属性基可搜索加密方案 [J]. 通信学报，2024, 45(9): 244-257.

[2] 潘雪，袁凌云，黄敏敏．主从链下的物联网隐私数据跨域安全共享模型 [J]. 计算机应用研究，2022, 39(11):3238-3243.

[3] 李井涵，沈国华，杨阳，等．结合区块链的物联网数据安全共享机制 [J]. 小型微型计算机系统，2023, 44(8):1812-1818.

[4] 张学旺，陈思宇，罗欣悦，等．面向云辅助工业物联网的高效可搜索属性基加密方案 [J]. 信息网络安全，2024, 24(9): 1352-1363.

[5] 郝旭龙，董国芳．基于联盟链和属性加密的智能电网数据共享方案 [J]. 云南民族大学学报（自然科学版），2023, 32(3): 352-358.

[6] 黄磊，易文姣，王英，等．基于联邦学习和多方安全计算的海铁联运数据安全共享方法研究 [J]. 铁道运输与经济，2024, 46(4): 58-67.

[7] 刘雪娇，曹天聪，夏莹杰．区块链架构下高效的车联网跨域数据安全共享研究 [J]. 通信学报，2023, 44(3): 186-197.

[8] 王瑞民，吴佳璇，张建辉．基于秘密分割的区块链安全数据共享模型 [J]. 重庆邮电大学学报（自然科学版），2023, 35(6): 1145-1153.

[9] 黄杨杨．属性 Logistic 混沌映射下的物联网隐私数据安全共享 [J]. 现代电子技术，2024,47(13):97-101.

[10] 申童童，黄保华．基于 Fabric 和属性加密的数据安全共享方案 [J]. 广西大学学报（自然科学版），2024, 49(3): 585-594.

【作者简介】

赵治斌（1975—），男，甘肃临洮人，硕士，副教授，研究方向：计算机网络技术、物联网技术。

冯黎（1979—），女，甘肃临洮人，硕士，副教授，研究方向：计算机技术。

（收稿日期：2024-12-04）