引用格式：刘春, 张凌浩, 蒋昌松, 等. 基于联盟链的电力数据安全存储与访问控制方案 [J]. 电子科技大学学报, 2026, 55(3): 455-463.
LIU C, ZHANG L H, JIANG C S, et al. Consortium blockchain-based secure storage and access control of power data[J]. Journal of University of Electronic Science and Technology of China, 2026, 55(3): 455-463.

基于联盟链的电力数据安全存储与访问控制方案

刘 春[1]，张凌浩[2]，蒋昌松[3*]，周 轩[1]，张 琴[1]，许春香[4]

（1. 国网四川省电力公司乐山供电公司，乐山 614000；2. 国网四川省电力公司电力科学研究院，成都 610000；
3. 电子科技大学信息与软件工程学院，成都 610054；4. 电子科技大学计算机科学与工程学院，成都 611731）

摘要：随着电力行业数字化转型和智能电网技术的深入发展，电力系统中产生的大规模数据对安全存储与高效访问提出了更高要求。传统存储模式存在监管困难、溯源效率低等问题。为此，该文提出了一种基于联盟链的电力数据安全存储与访问控制方案。构建了一种链上链下相结合的电力数据存储模式，将电力数据加密后存储在存储服务器，并利用联盟链记录关键信息，确保了数据的机密性、不可篡改性和可追溯性。利用布隆过滤器和对称加密设计了一种支持关键字检索的加密存储方法，在保证数据安全存储的同时，实现了高效的数据检索，提升了系统的实用性。此外，基于智能合约和盲签名实现了基于用户属性的访问控制，实现细粒度的权限管理，确保数据访问的安全性和灵活性。同时提供了形式化的安全性分析，证明所提方案在保证关键字安全性的同时能抵抗冒充攻击和窃听攻击。性能分析表明，与现有方案相比，所提方案在数据搜索阶段将计算开销降低了 68%，在数据访问阶段将通信开销降低了 37%。

关键词：电力数据；联盟链；安全存储；访问控制
中图分类号：TP309 **文献标志码：**A DOI: 10.12178/1001-0548.2025016

Consortium blockchain-based secure storage and access control of power data

LIU Chun[1], ZHANG Linghao[2], JIANG Changsong[3*], ZHOU Xuan[1], ZHANG Qin[1], and XU Chunxiang[4]

(1. State Grid Sichuan Electric Power Company Leshan Power Supply Company, Leshan 614000, China;
2. State Grid Sichuan Electric Power Research Institute, Chengdu 610000, China;
3. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China;
4. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: With the digital transformation of the power industry and the widespread adoption of smart grid technologies, the massive volume of data generated within power systems has imposed higher demands on secure storage and efficient access. However, traditional data storage models face challenges, such as difficulties in regulatory supervision and low efficiency in data traceability. To address these issues, this paper proposes a secure storage and access control scheme for power data based on consortium blockchains. In this scheme, a hybrid storage model combining on-chain and off-chain mechanisms is established, the encrypted power data is stored in the storage server, and the key information is recorded on the consortium blockchain, which ensures data confidentiality, immutability, and traceability. An encrypted data storage method supporting keyword search is designed by Bloom filters and symmetric encryption. While ensuring the secure storage of data, the designed method achieves efficient data retrieval and enhances the practicality of systems. Moreover, smart contract and blind signature are utilized to achieve user attribute-based access control, which achieves fine-grained permission management and ensures the security and flexibility of data access. A formal security analysis demonstrates that the proposed scheme can effectively resist impersonation and eavesdropping attacks while ensuring the security of keyword information. Performance evaluation shows that, compared with existing schemes, the proposed solution reduces computational overhead by 68% during the data search phase and lowers communication overhead by 37% during the data access phase.

收稿日期：2025−01−15
基金项目：国网四川省电力公司科技项目资助（521908230001）
作者简介：刘春，主要从事网络与数据安全、电力物联网、电力数据应用等方面的研究。
*通信作者 E-mail: jiangchso@163.com

Key words: power data; consortium blockchain; encrypted storage; access control

随着电力数据量的快速增长和应用场景的多样化，传统的数据管理模式已难以满足智能电网对数据安全性和可靠性的高要求。当前电力数据管理在实践中面临数据监管困难和溯源效率较低等挑战。具体而言，由于电力数据涵盖多个环节和参与方，不同主体的数据访问权限和使用合规性需要精细化管理，增加了监管复杂性。此外，电力数据在生成、传输和使用过程中涉及多个系统和平台，跨部门或跨系统的数据追踪面临一致性和时效性不足的问题。为了解决这些问题，区块链技术因其不可篡改性、数据透明性以及操作可追溯性等优势，逐渐成为电力数据管理的重要研究方向之一。

现有基于区块链的电力数据存储方案利用区块链技术来存储和管理数据。文献 [1] 结合区块链和基于密文策略的属性基加密技术，构建了云端数据共享方案，确保上链数据的不可修改性。文献 [2] 提出了针对车联网数据安全和访问控制的区块链数据共享方案。文献 [3] 探讨了利用区块链和代理重加密技术的数据共享方案，社交网络数据共享方案中，区块链通常被用于防止数据篡改。文献 [4] 结合区块链和二叉树技术实现属性的防篡改性。文献 [5] 提出了基于区块链的跨部门密文数据共享模型，但计算效率较低。此外，多项方案[6-9] 使用了区块链技术，但大多数方案侧重于访问用户的计算性能，忽视了数据拥有者的计算负担。这些方案应用在资源有限的数据采集设备中时存在局限性，需要进一步优化。

文献 [10] 设计了轻量级的城市区块链交易网络，用于记录城市中公共电力设施与电动汽车之间的频繁电力交易数据。然而，这些系统通常对大多数用户开放数据验证，缺乏可靠的控制机制来保障隐私交易数据的安全访问。文献 [11] 提出了微电网数据安全共享方案，要求用户注册并广播打包好的数据区块，通过积分替代传统区块链共识机制中的代币流通，将个体的太阳能发电转化为公共电力服务。然而，这些系统未充分考虑个人隐私，公开个人电力交易数据可能导致数据安全风险。基于区块链的数据流转访问控制[12-14] 和电力数据跨部门交换共享机制[15-20] 也进行了相关探究。

尽管现有研究结合区块链技术提出了多种方案，但在检索效率和细粒度访问控制方面仍有所不足。首先，为了保障数据的安全性，数据在存储前通常需要进行加密。然而，传统的加密算法（如 AES）会阻碍密文数据的搜索，且对区块链上的数据进行关键字检索效率较低，这将显著制约方案的实际应用和部署。其次，现有方案通常缺乏细粒度的访问控制。电力数据在存储过程中通常需要进行分级分类，数据等级越高，隐私性要求越强，对访问用户的要求也越高。因此，如何在电力数据访问过程中设计有效的细粒度访问控制机制，成为亟待解决的关键问题。

为了解决上述问题，本文提出了一种基于联盟链的电力数据安全存储与访问控制方案，旨在实现电力数据的安全存储和高效检索。具体而言，本文研究了一种链上链下相结合的电力数据存储机制，其中电力数据密文存储于链下的电力数据库，密钥由一个代理服务器管理，实现安全可靠的数据存储。用户名、存储记录、数据哈希值和数据签名等关键信息则通过智能合约存储于联盟链上，以确保数据的不可篡改性、可追溯性和认证性。为了保证高效的数据检索，本文基于布隆过滤器和对称加密技术设计了一种支持关键字检索的加密存储方法，使得数据在加密状态下仍能被高效检索和访问。这种方法不仅确保了数据的安全性，还提升了检索效率和系统实用性。

当用户执行数据访问时，用户首先需要与认证服务器认证自己的身份，并获得认证服务器颁发的令牌。该令牌颁发基于 BLS 盲签名进行构建，保证用户的口令安全性。随后用户使用令牌向代理服务器认证自己的身份。令牌中包含用户特有的属性信息（如身份、职务等），一旦用户持有的令牌属性满足相应文件的访问要求，代理服务器便进行密文检索，并将检索得到的数据返回给用户。该方式有效实现了细粒度的数据访问权限管理和数据使用监管。

1 基础知识

1.1 联盟链

联盟链（consortium blockchain）是一种介于公有链和私有链之间的区块链类型[21]。它由多个组织或机构共同管理和使用，参与的成员需要经过授权才能加入区块链网络。这种结构既保留了区块链去中心化的特点，又提供了更高的隐私性和可控性，特别适合跨组织的业务协作和数据共享。联盟链是由一组预选节点共同维护和管理的区块链网

络。与公有链不同，联盟链的参与者是有限的，只有获得授权的节点才能加入网络并访问链上的数据。联盟链的主要特点包括授权访问、去中心化、高效性和隐私性。授权访问确保只有经过许可的成员可以参与链上活动；去中心化则由多个独立的实体共同维护，提升系统的可靠性；高效性体现在其共识机制通常更为高效，交易处理速度更快；隐私性则通过限制访问权限来保障数据安全。

1.2　智能合约

智能合约（smart contract）是一种自执行的协议，具有合约条款直接写入代码中的特性。它可以在区块链上自动执行并管理合约的各项条款和条件，无需人工干预。智能合约的目的是减少信任成本、提高交易效率和安全性。在区块链系统中，智能合约被部署在区块链上，运行在特定的区块链虚拟机中（如以太坊虚拟机 EVM）。智能合约的账户通常分为两类：外部账户和合约账户。外部账户由用户控制，使用私钥签名交易；而合约账户由智能合约控制，通过代码执行特定功能。

智能合约的执行依赖于区块链上的交易。用户通过发送交易触发智能合约的执行，这些交易包含调用合约的指令和所需参数。当交易被发送到区块链网络时，矿工会打包这些交易并将其包含在新区块中。矿工通过解决复杂的数学问题来验证交易，这个过程被称为挖矿。挖矿不仅确保了交易的有效性，还维持了区块链的去中心化和安全性。矿工解决数学问题后，验证交易并将新区块添加到区块链中，随后这些交易会被智能合约执行。智能合约根据交易中包含的指令和参数自动执行相应的操作，并将结果记录在区块链上。

1.3　布隆过滤器

布隆过滤器是一种高效的空间节省数据结构，用于快速判断一个元素是否属于某个集合[22]。具体而言，布隆过滤器包含一个数组和多个哈希函数。给定一个元素，布隆过滤器将元素的哈希值映射到数组的多个位置，并将这些位置的位设为 1。查询时，如果所有相关位均为 1，则元素在集合中；否则元素不在集合中。尽管布隆过滤器可能会存在假阳性的情况，但其空间和时间效率使其适合大规模数据集的处理。

1.4　双线性映射

假设G是阶为素数p的加法循环群，G_T是阶为p的乘法循环群，双线性映射$e:G\times G\to G_T$满足以下性质。

1）双线性性：对于任意$A,B\in G,a,b\in Z_p^*$，满足$e(aA,bB)=e(A,B)^{ab}$；

2）非退化性：存在$X,Y\in G$，满足$e(X,Y)\neq 1_{G_T}$；

3）可计算性：对于任意$M,N\in G$，计算$e(M,N)$是高效的。

1.5　BLS 盲签名

假设$e:G\times G\to G_T$是一个双线性映射，$H:\{0,1\}^*\to G$是一个哈希函数，P为群G的生成元。BLS 盲签名由以下算法构成。

1）密钥生成：生成私钥$x\in Z_p^*$和公钥$\mathrm{pk}=xP$；

2）消息盲化：给定消息m，计算$M=H(m)$，随机选择$r\in Z_p^*$，计算盲化消息$M'=rM$；

3）签名生成：给定盲化消息M'，计算盲化签名$\sigma'=xM'$；

4）去盲：给定盲化签名σ'，计算签名$\sigma=r^{-1}\sigma'$；

5）签名验证：给定签名σ，验证其是否满足$e(\sigma,P)=e(H(m),\mathrm{pk})$；

BLS 盲签名满足盲化性和不可伪造性[23]。

2　问题描述

2.1　系统模型

基于联盟链的电力数据安全存储与访问控制方案，包括代理服务器、存储服务器、认证服务器和用户。系统模型如图 1 所示。

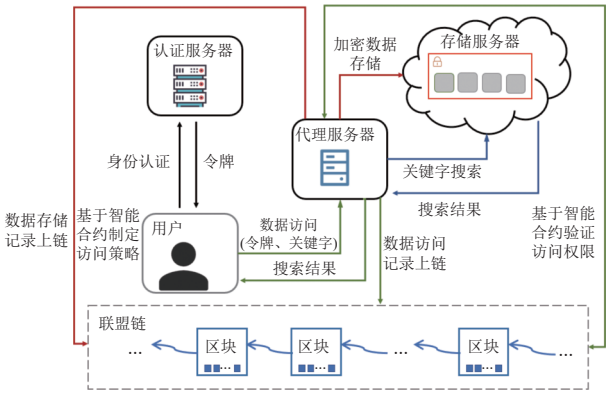


图 1　系统模型

1）代理服务器：负责加密数据存储，并通过用户发送的令牌验证其身份的合法性。一旦用户满足数据访问策略，代理服务器将协助其进行关键字搜索并返回存储服务器发送的搜索结果。相应的数据存储记录、访问权限验证、数据访问记录等将通过智能合约存储于联盟链上。

2）存储服务器：为用户提供数据存储服务。此外，它在收到代理服务器发送的关键字搜索查询时，将进行数据检索，并将检索得到的结果回信给

代理服务器。

3）认证服务器：为用户提供认证服务。一旦用户通过身份认证，将为其颁发令牌。

4）用户：在认证服务器处认证身份，并使用获取的令牌向代理服务器请求关键字数据搜索。

2.2 威胁模型

本文的威胁模型考虑两类敌手：外部敌手和内部敌手。

外部敌手：可能发起冒充攻击，冒充用户向认证服务器请求令牌。此外，外部敌手可能发起窃听攻击，窃听传输的消息以试图得到用户口令或外包数据。

内部敌手：为半诚实的存储服务器，其诚实地执行数据存储、关键字检索等操作，但可能会试图从接收到的消息中获取关键字等信息。

3 方案介绍

3.1 方案概述

该方案涉及代理服务器$\mathcal{PS}$、存储服务器$\mathcal{SS}$、认证服务器$\mathcal{AS}$和用户$\mathcal{U}$，共包含 4 个阶段：系统初始化阶段、数据存储阶段、身份认证阶段和数据访问阶段。

系统初始化阶段：根据安全参数确定系统公共参数集。

数据存储阶段：给定一个数据集DB，代理服务器$\mathcal{PS}$将DB进行加密，存储在存储服务器$\mathcal{SS}$上，以便在密文数据上执行关键字检索。相应的存储记录在联盟链上。此外，$\mathcal{PS}$通过区块链智能合约制定关于数据集的访问策略。

身份认证阶段：由注册步骤和认证步骤两部分组成。用户$\mathcal{U}$首先向认证服务器$\mathcal{AS}$进行注册，$\mathcal{AS}$存储$\mathcal{U}$的身份标识$\mathrm{ID}_{\mathcal{U}}$和包含用户属性的注册信息RI。$\mathcal{U}$在$\mathcal{AS}$处完成身份认证后，将获得用于数据访问的认证令牌。

数据访问阶段：假设用户想访问数据集DB并检索包含关键字w的数据记录。代理服务器$\mathcal{PS}$将验证$\mathcal{U}$发送的令牌tkn的有效性，并通过智能合约验证用户属性是否满足DB的访问策略。若验证均通过，则在存储服务器$\mathcal{SS}$的帮助下检索目标数据并将其发送给$\mathcal{U}$，否则拒绝此次访问请求。相应的数据访问记录将通过智能合约存储于联盟链上。

3.2 方案设计

3.2.1 系统初始化阶段

根据安全参数l确定系统公共参数集$\{p,P,G,G_T,e,\mathrm{Enc},\mathrm{Dec},F,H,h,\mathrm{Insert},\mathrm{Lookup}\}$，其中$G$是阶为素数$p$、生成元为$P$的加法循环群，$G_T$是阶为$p$的乘法循环群，$e:G\times G\to G_T$是一个双线性映射，Enc是一个安全的对称加密算法，Dec是相应的解密算法，$F:\{0,1\}^l\times\{0,1\}^*\to\{0,1\}^l$是一个安全的伪随机函数，$H:\{0,1\}^*\to G$、$h:\{0,1\}^*\to\{0,1\}^l$是两个抗碰撞的哈希函数，Insert可以将一个数据项x插入布隆过滤器BF中，Lookup可以查询数据项x是否包含在BF里面。认证服务器$\mathcal{AS}$生成签名密钥$s_{\mathcal{AS}}\in Z_p^*$和验证密钥$Q_{\mathcal{AS}}=g^{s_{\mathcal{AS}}}$。

3.2.2 数据存储阶段

给定一个数据集$\mathrm{DB}=\{\mathrm{id}_i,W_i\}_{i\in[d]}$，其中DB的每条数据记录由标识符$\mathrm{id}_i\in\{0,1\}^*$和关键字集$W_i\in\{0,1\}^*$构成。代理服务器$\mathcal{PS}$将DB进行加密，存储在存储服务器$\mathcal{SS}$上，以便在密文数据上执行关键字检索。此外，$\mathcal{PS}$通过区块链智能合约制定关于数据集DB的访问策略。具体过程如下所示。

1）$\mathcal{PS}$随机选择密钥$K\in\{0,1\}^l$，初始化一个列表L和一个布隆过滤器BF；

2）对于每个关键字$w\in\cup_{i=1}^{d}W_i$，$\mathcal{PS}$执行如下操作：

① 使用K计算密钥$K_1=F(K,w\|1)$和$K_2=F(K,w\|2)$，并初始化一个计数器$c=0$；

② 对于每个标识符$\mathrm{id}\in\{\mathrm{id}_i:w\in W_i\}$，$\mathcal{PS}$使用密钥$K_1$和计数器$c$计算一个伪随机标签$\mathrm{rl}=F(K_1,c)$，使用$K_2$加密id得到密文$\mathrm{eid}=\mathrm{Enc}(K_2,\mathrm{id})$；

③ $\mathcal{PS}$将计数器c加 1，将$(\mathrm{rl},\mathrm{eid})$添加到列表$L$中，并执行$\mathrm{Insert}(\mathrm{rl},\mathrm{BF})$；

3）$\mathcal{PS}$使用列表L创建一个字典γ（给定rl，γ会返回对应的eid）；

4）$\mathcal{PS}$使用密钥K加密每个数据记录，随后将字典γ及所有数据记录密文C发送给存储服务器$\mathcal{SS}$；

5) $\mathcal{SS}$将收到的消息进行链下存储。相应的数据存储记录$(\mathrm{ID}_{\mathrm{DB}},h(\gamma),h(\mathrm{BF}),h(C))$将通过智能合约存储在联盟链上，其中$\mathrm{ID}_{\mathrm{DB}}$表示数据集DB的标识；

6）$\mathcal{PS}$生成关于数据集DB的访问策略：访问者（即用户）在通过身份认证的同时必须具备属性集$\mathrm{AT}_{\mathrm{req}}$。$\mathcal{PS}$通过智能合约将该访问策略上传至联盟链上，使得给定一个属性集AT，智能合约可以检查$\mathrm{AT}\in\mathrm{AT}_{\mathrm{req}}$是否成立。若成立，则执行数据访问阶段，否则拒绝。

3.2.3　身份认证阶段

身份认证阶段由注册步骤和认证步骤两部分组成。用户$\mathcal{U}$首先向认证服务器$\mathcal{AS}$进行注册，$\mathcal{AS}$存储$\mathcal{U}$的身份$\mathrm{ID}_{\mathcal{U}}$和注册信息RI。$\mathcal{U}$在$\mathcal{AS}$处成功认证身份后，将获得用于数据访问的认证令牌tkn。具体过程如下所示。

注册步骤：

1）用户$\mathcal{U}$选择用户名$\mathrm{ID}_{\mathcal{U}}$和口令$\mathrm{pw}_{\mathcal{U}}$，并随机选择注册密钥$k \in Z_p^*$；

2）$\mathcal{U}$计算凭证$\mathrm{cred} = h(kH(\mathrm{pw}_{\mathcal{U}})\|\mathrm{pw}_{\mathcal{U}})$，其中$\|$表示字符串连接。$\mathcal{U}$通过安全信道发送$\left(\mathrm{ID}_{\mathcal{U}}, k, \mathrm{cred}, \left\{\mathrm{att}_j\right\}_{j\in[n]}\right)$给认证服务器$\mathcal{AS}$，其中$\left\{\mathrm{att}_j\right\}_{j\in[n]}$表示用户$\mathcal{U}$的$n$个属性（如性别、职务）；

3）认证服务器$\mathcal{AS}$秘密存储用户$\mathcal{U}$的注册信息$\left(\mathrm{ID}_{\mathcal{U}}, k, \mathrm{cred}, \left\{\mathrm{att}_j\right\}_{j\in[n]}\right)$。

认证步骤：

1）用户$\mathcal{U}$使用随机数$r \in Z_p^*$计算盲化口令$\mathrm{pw}_{\mathcal{U}}^* = rH(\mathrm{pw}_{\mathcal{U}})$；

2）$\mathcal{U}$发送认证请求$\mathrm{req} = (\mathrm{ID}_{\mathcal{U}}, \mathrm{pw}_{\mathcal{U}}^*)$给认证服务器$\mathcal{AS}$；

3）认证服务器$\mathcal{AS}$收到$\mathrm{req} = (\mathrm{ID}_{\mathcal{U}}, \mathrm{pw}_{\mathcal{U}}^*)$后，使用$\mathrm{ID}_{\mathcal{U}}$对应的注册密钥$k$处理盲化口令$\mathrm{pw}_{\mathcal{U}}^*$得到$\sigma^* = k\mathrm{pw}_{\mathcal{U}}^*$，并使用签名密钥$s_{\mathcal{AS}}$生成令牌$\mathrm{tkn} = s_{\mathcal{AS}}H\left(\mathrm{ID}_{\mathcal{U}}\|\left\{\mathrm{att}_j\right\}_{j\in[n]}\|\mathrm{ext}\right)$，其中ext表示令牌的有效截止日期；

4）$\mathcal{AS}$计算密文$\mathrm{etkn} = \mathrm{Enc}\left(\mathrm{cred}, \mathrm{tkn}\|\left\{\mathrm{att}_j\right\}_{j\in[n]}\|\mathrm{ext}\right)$，发送认证响应$\mathrm{res} = (\sigma^*, \mathrm{etkn})$给$\mathcal{U}$；

5）$\mathcal{U}$收到$\mathrm{res} = (\sigma^*, \mathrm{etkn})$后，计算凭证$\mathrm{cred} = h(r^{-1}\sigma^*\|\mathrm{pw}_{\mathcal{U}})$，使用cred解密etkn得到令牌tkn、属性$\left\{\mathrm{att}_j\right\}_{j\in[n]}$和有效截止日期ext。

3.2.4　数据访问阶段

假设用户$\mathcal{U}$想访问数据集DB并检索包含关键字w的数据记录。代理服务器$\mathcal{PS}$将验证$\mathcal{U}$发送的令牌tkn的有效性以及用户属性是否满足DB的访问策略。若验证均通过，则在存储服务器$\mathcal{SS}$的帮助下检索数据并将其发送给$\mathcal{U}$，否则拒绝此次访问请求。

1）$\mathcal{U}$发送访问请求$\mathrm{req}' = \left(\mathrm{ID}_{\mathcal{U}}, \mathrm{tkn}, \left\{\mathrm{att}_j\right\}_{j\in[n]}, \mathrm{ext}, w\right)$给代理服务器$\mathcal{PS}$；

2）代理服务器$\mathcal{PS}$通过检验等式$e(\mathrm{tkn}, P) = e\left(H(\mathrm{ID}_{\mathcal{U}}\|\left\{\mathrm{att}_j\right\}_{j\in[n]}\|\mathrm{ext}), Q_{\mathcal{AS}}\right)$是否成立来验证令牌tkn的有效性。此外，$\mathcal{PS}$通过智能合约验证$\left\{\mathrm{att}_j\right\}_{j\in[n]} \in AT_{\mathrm{req}}$是否成立。若任一验证不通过，则拒绝此次访问请求。若验证均通过，则计算密钥$K_1 = F(K, w\|1)$和$K_2 = F(K, w\|2)$，发送(K_1, K_2)给存储服务器$\mathcal{SS}$用于关键字密文检索；

3）存储服务器$\mathcal{SS}$初始化计数器$c = 0$，计算伪随机标签$\mathrm{rl} = F(K_1, c)$，通过$\mathrm{Lookup}(\mathrm{rl}, \mathrm{BF})$验证rl是否存在于布隆过滤器BF中。若存在，则从字典γ中获取rl对应的密文eid，并使用K_2解密eid得到$\mathrm{id} = \mathrm{Dec}(K_2, \mathrm{eid})$；

4）令L为得到的id集合。$\mathcal{SS}$发送对应的数据记录密文C_L给$\mathcal{PS}$；

5）$\mathcal{PS}$解密数据记录密文C_L，得到的数据记录安全地发送给$\mathcal{U}$。$\mathcal{PS}$通过智能合约将访问记录$\left(\mathrm{ID}_{\mathcal{U}}, \mathrm{ID}_{\mathrm{DB}}, \mathrm{time}, h(\mathrm{tkn}\|\left\{\mathrm{att}_j\right\}_{j\in[n]}\|\mathrm{ext})\right), h(C_L), h(K_1\|K_2))$上链，其中time表示当前时间；

7）$\mathcal{U}$得到数据集DB中包含关键字w的数据记录，完成本次数据访问。

3.3　方案正确性证明

在身份认证阶段的认证步骤中，凭证$\mathrm{cred} = h(r^{-1}\sigma^*\|\mathrm{pw}_{\mathcal{U}}) = h(r^{-1}k\mathrm{pw}_{\mathcal{U}}^*\|\mathrm{pw}_{\mathcal{U}}) = h(r^{-1}k\ rH(\mathrm{pw}_{\mathcal{U}})\|\mathrm{pw}_{\mathcal{U}}) = h(kH(\mathrm{pw}_{\mathcal{U}})\|\mathrm{pw}_{\mathcal{U}})$。因此，当用户输入正确的口令$\mathrm{pw}_{\mathcal{U}}$时，可以生成与注册阶段一致的凭证，以此完成身份认证。此外，当用户通过认证后，代理服务器可以计算密钥K_1和K_2来协助存储服务器完成关键字检索。

4　安全性分析

所提方案可以防止外部敌手和内部敌手（即半诚实的存储服务器）获取任何关键字信息。

抵御内部敌手：在数据存储阶段，代理服务器使用伪随机函数从密钥K派生出针对每个关键字w的密钥K_1和K_2，K_1用于计算伪随机标签，K_2用于加密数据记录标识符。伪随机函数的安全性保证了存储服务器无法通过K_1和K_2计算密钥K和关键字w，并且无法通过伪随机标签计算K_1。

本文采用真实/理想模拟范式（real/ideal simulation paradigm）进行关键字安全性分析。首先设定两个游戏：$\mathrm{SSEReal}(l)$和$\mathrm{SSESimL}(l)$。在第 1 个游戏$\mathrm{SSEReal}(l)$中，敌手$\mathcal{A}$选择 1 个数据库作为输入并接收协议运行得到的字典γ，然后可以自适应地执行关键字查询和搜索预言机，游戏按照协议执行返还相应的结果。游戏最后输出由$\mathcal{A}$选择的比特b。第 2 个游戏$\mathrm{SSESimL}(l)$不再返还协议执行得到的结

果，而是返还仿真者S仿真的结果。游戏最后输出由$\mathcal{A}$选择的比特b。如果敌手区分这两个游戏的概率是可忽略的，则所提方案能够保证关键字的安全性。

定理 1 所提方案可以保证关键字的安全性，当且仅当对于任意概率多项式时间（PPT）敌手$\mathcal{A}$，存在一个 PPT 仿真者S，使得$\mathrm{Adv}_{\mathcal{A}} = \Pr[\mathrm{SSEReal}(l)=1]-\Pr[\mathrm{SSESimL}(l)=1]$是可忽略的。

证明：该定理采用混合论据（hybrid argument）方式进行证明。下面将展示如何通过一系列的游戏转换将协议的真实执行（$\mathrm{SSEReal}(l)$）转换为完全仿真的执行（$\mathrm{SSESimL}(l)$）。

游戏 G_0：该游戏为$\mathrm{SSEReal}(l)$。

游戏 G_1：该游戏与游戏G_0的唯一区别在于通过维护一个列表T来模拟$F(K,\cdot)$的执行。对于输入x，如果x不属于T，则S随机选择$K_1\|K_2\in\{0,1\}^{2l}$，将其存储在T中并返回$K_1\|K_2$，否则直接从T中检索并返回对应的$K_1\|K_2$。由于伪随机函数的安全性，该游戏与游戏G_0是不可区分的。

游戏 G_2：该游戏与游戏G_1的唯一区别在于改变了标签rl的生成方式。具体来说，若敌手$\mathcal{A}$查询过关键字w，则按照$\mathrm{rl}=F(K_1,c)$来计算，否则S随机选择$\mathrm{rl}\in\{0,1\}^l$。对于第 1 种方式而言，K_1是随机选取的，因此rl对于敌手$\mathcal{A}$来说是均匀随机的。显然第 2 种方式对于$\mathcal{A}$而言也是均匀随机的。因此，可以得到游戏G_2和G_1是不可区分的。

游戏 G_3：该游戏与游戏G_2的不同之处在于，若敌手$\mathcal{A}$未查询过关键字w，S使用随机选择的K_2加密的相同长度的 0 比特串（而不是执行$\mathrm{eid}=\mathrm{Enc}(K_2,\mathrm{id})$）。由于对称加密算法的选择明文攻击（CPA）安全性，游戏G_3和G_2是不可区分的。

此时，游戏G_3便是$\mathrm{SSESimL}(l)$。根据上述分析，定理 1 得证。

抵御外部敌手：接下来将证明用户口令的安全性。由于在注册过程中，用户通过安全信道将注册信息发送给认证服务器，因此本文仅考虑认证过程中的口令安全性。

定理 2 所提方案可以防止外部敌手冒充用户。

证明：用户使用口令向身份服务器认证身份，由于敌手没有用户口令，因此无法进行用户冒充。考虑敌手可能在用户认证身份时通过窃听攻击获取用户口令这一威胁。在所提方案中，用户使用了 BLS 盲签名生成凭证$\mathrm{cred}=h(kH(\mathrm{pw}_{\mathcal{U}})\|\mathrm{pw}_{\mathcal{U}})$，用于解密密文etkn得到令牌等信息。BLS 盲签名的盲化性[21]确保了认证过程不会泄露口令的任何信息。

5 性能评估

5.1 方案实现

本文实现了基于联盟链的电力数据安全存储与访问控制方案，使用 JAVA 语言和密码学库 crypto 实现了密码学操作。使用 Ganache 实现区块链，并通过 web3j 与区块链进行通信，采用 Type A 曲线$y^2=x^3+x$实现双线性映射，同时使用 AES-CRT 实现对称加密，并基于 SHA-256 实现了哈希函数和伪随机函数。安全参数选取为 80 bits。因此可以得到$|Z_p^*|=160$ bits 和$|G|=1\,024$ bits。实验硬件参数为 Intel(R) Core(TM) i7-8750H CPU 2.20 GHz、16 GB RAM，操作系统为 Windows10 系统。

所提方案的实现主要涉及认证服务器、用户和代理服务器。三者间的交互如图 2 所示。

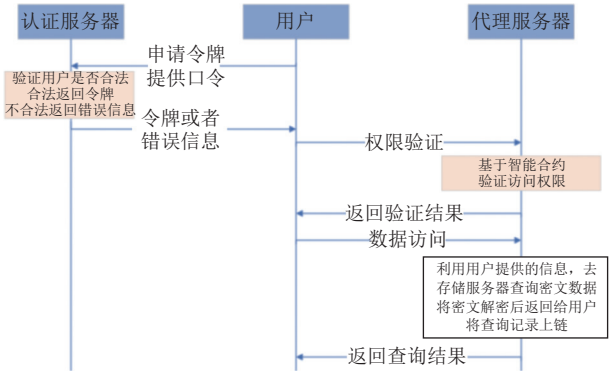


图 2 认证服务器、用户和代理服务器间的交互

5.2 计算开销

在身份认证阶段，用户计算盲化口令，随后对认证服务器返回的签名进行去盲化，主要计算开销为$\mathrm{Hash}_G+2\mathrm{Mul}$，其中$\mathrm{Hash}_G$表示将任意字符串映射到群$G$中，Mul表示群$G$中的乘法运算。认证服务器生成签名和令牌，主要计算开销为$\mathrm{Hash}_G+2\mathrm{Mul}$。在数据存储阶段，代理服务器针对每个关键字进行密钥派生，并使用对称加密算法加密数据记录及其标识符，总体计算开销随着数据记录数量和关键字数量呈线性增长。在数据访问阶段，代理服务器通过双线性映射验证令牌的有效性、计算用于检索的密钥并解密存储服务器发送的密文。存储服务器计算伪随机标签rl、验证rl是否在布隆过滤器中并解密检索得到的标识符密文。

图 3 展示了认证阶段与数据访问阶段中认证服

务器和代理服务器的计算开销，其中假设代理服务器检索并解密 100 条数据记录密文。开销随着用户数量线性增加，但整体开销保持在可接受范围内。即使用户数量从 100 增加到 700，认证服务器的开销仅增长至 14 s，代理服务器增长至 17.5 s，表明该方案在扩展性和计算效率方面具备良好的性能，能够满足大规模用户场景下的需求。

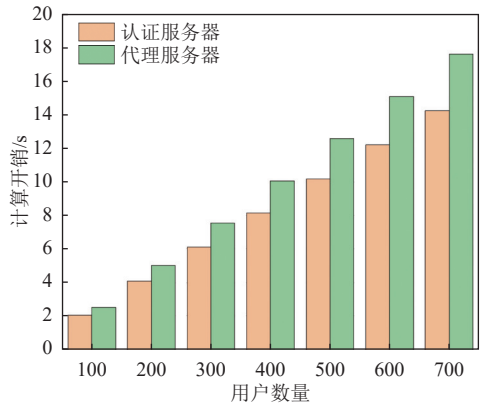


图 3　认证与数据访问阶段服务器计算开销

图 4 展示了代理服务器将数据存储记录上链的计算开销，其中假设每个用户访问代理服务器只上链一条消息。开销随着用户数量线性增加，但整体开销保持在可接受范围内。实验结果表明，即使用户数量达到 700，代理服务器的总开销低于 15 s。

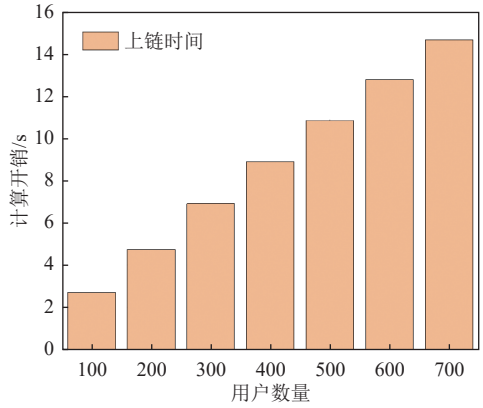


图 4　代理服务器计算开销

在数据搜索阶段，本文方案的代理服务器利用主密钥和关键字生成两个子密钥，主要计算开销为 $2F$，其中 F 表示伪随机函数。存储服务器通过子密钥计算伪随机标签，然后查询字典获取密文，最后解密得到结果，主要计算开销为 $n(F+\text{Get}+\text{Dec})$，其中 n 表示包含关键字的文件数量，Get 表示查询字典，Dec 表示解密。在现有方案 MITRA[24] 中，用户通过关键字计算伪随机标签，主要计算开销为 $n(F+\text{Add})$，其中 Add 表示添加进列表。存储服务器查询字典获取密文，主要开销为 $n(\text{Get}+\text{Add})$。最后用户解密得到结果，主要开销为 $n\text{Dec}$。在现有方案 Bestie[25] 中，用户通过关键字获取该关键字的更新次数、密钥以及索引，主要计算开销为 $n(\text{Map}+F+H)$，其中 Map 表示进行一次映射查找，H 表示哈希函数。存储服务器查询字典获取密文，主要开销为 $n(\text{Map}+H+\text{Add})$。最后用户解密得到结果，主要开销为 $n\text{Dec}$。

图 5 展示了数据访问阶段中本文所提方案与现有方案（MITRA 和 Bestie）在数据搜索阶段的计算开销对比情况。结果显示，所有方案的开销随着文件数量的增加而线性增加。当文件数量为 1 000 时，本文方案的开销约为 15 ms，相比于 MITRA 的 46 ms，降低了约 68%；相比于 Bestie 的 89 ms，降低了约 83%。造成这一差异的主要原因在于，本文方案在搜索过程中无需执行额外的添加操作，从而有效减少了计算负担。而 Bestie 的开销高于 MITRA，则主要源于其内部映射结构较为复杂，导致查找和处理过程更为耗时。与 MITRA 和 Bestie 相比，本文方案开销较低，表明该方案的高效性和实用性。

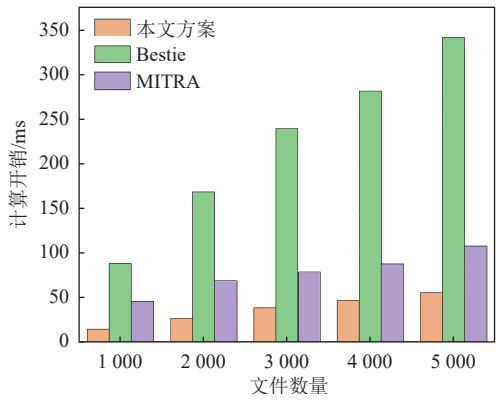


图 5　数据搜索阶段计算开销对比

5.3　通信开销

在数据存储阶段和数据检索阶段，代理服务器、用户与存储服务器通信开销与存储的（或检索的）数据量成正比。在身份认证阶段，用户与认证服务器的通信开销为 $|\text{ID}_{\mathcal{U}}|+3|G|+n|\text{att}|+|\text{ext}|$，其中 $|\text{ID}_{\mathcal{U}}|$、$|G|$、$|\text{att}|$、$n$和$|\text{ext}|$分别表示用户名$\text{ID}_{\mathcal{U}}$、群元素、属性、属性数和有效截止日期的大小。在实验中，$\text{ID}_{\mathcal{U}}$为 8 位字符串、$|\text{att}|=64$ bit、$|\text{ext}|=24$ bit。实验结果如图 6 所示。从图中可以看出，用户与认证服务器之间的通信开销随着用户数量和属性

数量的增加呈线性增长。当 $n=2,5,8$ 时，通信开销分别从 100 用户时的 40 KB、42 KB、45 KB，增加到 700 用户时的 281 KB、297 KB 和 314 KB。虽然开销随着用户数量和属性数量的增加有所上升，但增幅稳定且处于合理范围，表明该方案在面对较多用户和复杂属性时仍能保持较低的通信开销，具备良好的扩展性和适用性。

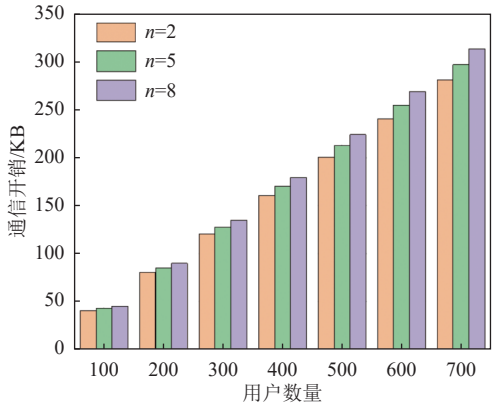


图 6 认证阶段用户与认证服务器通信开销

在数据访问阶段，本文方案中代理服务器与存储服务器的通信开销为密钥大小。而 MITRA 中用户和存储服务器之间的通信开销包含伪随机标签大小和密文大小；在 Bestie 中，则包含密钥大小和密文大小。实验仅考虑检索数据需要传输的消息，忽略了与认证相关的通信开销。在实验中，每个文件含有 2 个关键字，关键字长度为 8 位字符串。对比实验结果如图 7 所示。可以看出，本文方案的通信开销显著低于 MITRA 和 Bestie。当用户数为 1 000 时，本文所提方案通信开销约为 500 KB，相比 MITRA 的 1 500 KB，减少了约 66%；相比 Bestie 的 800 KB，减少了约 37%。通信开销降低的主要原因在于，本文方案在数据传输过程中仅需传送密钥，而无需传输密文。这一特点显著降低了对网络带宽和传输时间的要求，使得该方案在实际应用中更具部署优势。

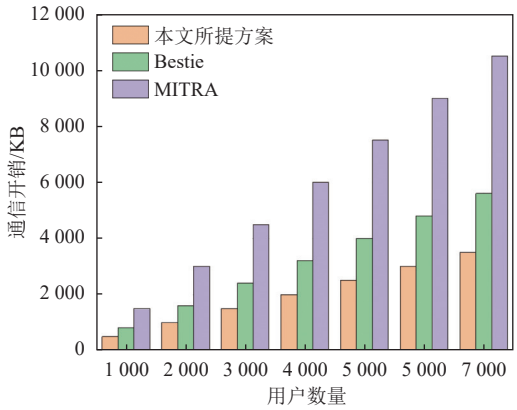


图 7 数据访问阶段通信开销对比

6 结束语

本文提出的基于联盟链的电力数据安全存储与访问控制方案，使用了一种链上链下相结合的电力数据存储模式，将电力数据加密后存储在存储服务器，并利用联盟链记录关键信息，确保了数据的机密性、不可篡改性和可追溯性。该方案使用了一种支持关键字检索的加密存储方法，在保证数据安全存储的同时，实现了高效的数据检索，提升了系统的实用性。此外，基于智能合约技术实现了基于用户属性的访问控制，实现细粒度的权限管理，确保数据访问的安全性和灵活性。本文分析了所提方案的安全性，并通过实验表明该方案在通信和计算方面的效率较高。

参 考 文 献

[1] ZUO Y T, KANG Z Z, XU J, et al. BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing[J]. International Journal of Distributed Sensor Networks, 2021, 17(3): 155014772199961.

[2] 杨颜博, 张嘉伟, 马建峰. 一种使用区块链保护车联网数据隐私的方法[J]. 西安电子科技大学学报, 2021, 48(3): 21-30.
YANG Y B, ZHANG J W, MA J F. Method for using the blockchain to protect data privacy of IoV[J]. Journal of Xidian University, 2021, 48(3): 21-30.

[3] 李雪莲, 张夏川, 高军涛, 等. 支持属性和代理重加密的区块链数据共享方案[J]. 西安电子科技大学学报, 2022, 49(1): 1-16.
LI X L, ZHANG X C, GAO J T, et al. Blockchain data sharing scheme supporting attribute and proxy re-encryption[J]. Journal of Xidian University, 2022, 49(1): 1-16.

[4] FAN K, PAN Q, ZHANG K, et al. A secure and verifiable data sharing scheme based on blockchain in vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5826-5835.

[5] 曾辉祥, 习宁, 谢晴晴, 等. 抗属性篡改的去中心化密文数据安全共享[J]. 西安电子科技大学学报, 2022, 49(2): 135-145.
ZENG H X, XI N, XIE Q Q, et al. Decentralized ciphertext sharing based on blockchain[J]. Journal of Xidian University, 2022, 49(2): 135-145.

[6] 尚松超, 陈勃翰, 颜光伟, 等. 基于区块链的数据共享访问控制模型[J]. 通信技术, 2021, 54(12): 2666-2673.
SHANG S C, CHEN B H, YAN G W, et al. Model for data sharing and access control based on blockchain[J]. Communications Technology, 2021, 54(12): 2666-2673.

[7] GODFREY W S, SIVA K A, RAMESH R. User centric block-level attribute based encryption in cloud using blockchains[J]. Computer Systems Science and

Engineering, 2022, 42(2): 605-618.
[8] ZHANG L Y, ZHANG T S, WU Q, et al. Secure decentralized attribute-based sharing of personal health records with blockchain[J]. IEEE Internet of Things Journal, 2022, 9(14): 12482-12496.
[9] XIANG X Y, ZHAO X W. Blockchain-assisted searchable attribute-based encryption for e-health systems[J]. Journal of Systems Architecture, 2022, 124: 102417.
[10] HASSIJA V, CHAMOLA V, GARG S, et al. A blockchain-based framework for lightweight data sharing and energy trading in V2G network[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5799-5812.
[11] ZHANG L H, CAO Y, ZHANG G Z, et al. A blockchain-based microgrid data disaster backup scheme in edge computing[J]. Security and Communication Networks, 2021, 2021: 9121571.
[12] ZHANG M, WANG S, ZHANG P, et al. Protecting data privacy for permissioned blockchains using identity-based encryption[C]//Proceedings of the IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference. [S.l.]: IEEE, 2019: 602-605.
[13] WANG Z, LIN J Q, CAI Q W, et al. Blockchain-based certificate transparency and revocation transparency[C]// Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2019: 144-162.
[14] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: Using blockchain to protect personal data[C]//Proceedings of the IEEE Security and Privacy Workshops. New York: IEEE, 2015: 180-184.
[15] 孙浩, 毛瀚宇, 张岩峰, 等. 区块链跨链技术发展及应用[J]. 计算机科学, 2022, 49(5): 287-295.
SUN H, MAO H Y, ZHANG Y F, et al. Development and application of blockchain cross-chain technology[J]. Computer Science, 2022, 49(5): 287-295.
[16] YIN Z Y, ZHANG B S, XU J Z, et al. Bool network: An open, distributed, secure cross-chain notary platform[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3465-3478.
[17] LIN S F, KONG Y H, NIE S T, et al. Research on cross-chain technology of blockchain[C]//Proceedings of the 6th International Conference on Smart Grid and Electrical Automation. [S.l.]: IEEE, 2021: 405-408.
[18] 张朝栋, 王宝生, 邓文平. 基于侧链技术的供应链溯源系统设计[J]. 计算机工程, 2019, 45(11): 1-8.
ZHANG C D, WANG B S, DENG W P. Design of supply chain traceability system based on side chain technology[J]. Computer Engineering, 2019, 45(11): 1-8.
[19] LI Z J, ZHANG Z H. Research and implementation of multi-chain digital wallet based on hash TimeLock [M]//Blockchain and Trustworthy Systems. Singapore: Springer Singapore, 2019: 175-182.
[20] 叶少杰, 汪小益, 徐才巢, 等. BitXHub: 基于侧链中继的异构区块链互操作平台[J]. 计算机科学, 2020, 47(6): 294-302.
YE S J, WANG X Y, XU C C, et al. BitXHub: Side-relay chain based heterogeneous blockchain interoperable platform[J]. Computer Science, 2020, 47(6): 294-302.
[21] JIANG C S, XU C X, CHEN J, et al. Blockchain-based immunization against kleptographic attacks[J]. Science China Information Sciences, 2024, 67(7): 172102.
[22] CHEN T Y, XU P, WANG W, et al. Bestie: Very practical searchable encryption with forward and backward security[C]//Computer Security–ESORICS 2021. Cham: Springer, 2021: 3-23.
[23] JIANG C S, XU C X, DONG X F, et al. An efficient privacy-preserving scheme for weak password collection in Internet of Things against perpetual leakage[J]. IEEE Transactions on Information Forensics and Security, 2024, 20: 1405-1420.
[24] GHAREH C J, PAPADOPOULOS D, PAPAMANTHOU C, et al. New constructions for forward and backward private symmetric searchable encryption[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 1038-1055.
[25] TARKOMA S, ROTHENBERG C E, LAGERSPETZ E. Theory and practice of bloom filters for distributed systems[J]. IEEE Communications Surveys & Tutorials, 2012, 14(1): 131-155.

责任编辑　叶　芳